C/M/S/

Law.Tax



CMS Guide to Data Privacy

July 2013

Austria	4
Belgium	8
Bulgaria	12
Croatia	16
Czech Republic	20
France	24
Germany	29
Hungary	33
Italy	38
Luxembourg	41
The Netherlands	44
Poland	48
Portugal	51
Romania	55
Russia	59
Serbia	63
Slovakia	66
Slovenia	70
Spain	74
Switzerland	78
Ukraine	82
United Kingdom	86

Introduction

Data privacy is everywhere around us. Social media, internet and e-mail usage of employees but also the transfer of data are all topics that play a role in companies nowadays. Data privacy has significant influence on many legal matters and therefore data privacy needs to be taken into account. Although the European Union is underpinned by common principles, considerable differences still remain, also in the area of data privacy. These differences are particularly noticeable in the development and application of labour laws.

This Guide provides an overview of data privacy laws in 21 European countries, including Russia. The Guide is intended to provide CMS's international clients, including those doing business across Europe, with a summary of local data privacy laws across all countries, making it easier to understand both the similarities and differences between each jurisdiction.

The Guide has been published by the CMS Employment and Pensions Practice Area Group, which comprises over 250 lawyers with specific expertise and experience in employment and pensions law, including data privacy. We are confident this Guide will be a valuable resource with respect to data privacy. If it encourages you to seek more detailed information, then please contact one of the members of the CMS Employment and Pensions Practice Area Group who will be happy to provide further advice. We have a proven track record in understanding our clients' needs and in delivering a professional and seamless service.

Katja van Kranenburg-Hanspians and Fernando Bázan López
CMS Practice Area Group Employment and Pensions

Austria



Group contact: Ursula Roberts

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	There are no laws regulating use of the internet at work for private purposes other than the Regulation of the Federal Government on the private use of information and communication technology infrastructure of the Federal Republic by public servants *(Verordnung der Bundesregierung über die private Nutzung der Informations- und Kommunikationstechnik-Infrastruktur des Bundes durch Bundesbedienstete* [IKT-Nutzungsverordnung – IKT-NV], BGBl. II Nr. 281/2009). In cases involving non-public employees, the employer has the right to decide whether employees may use the internet for private purposes or not, and to restrict access to the internet. In practice, use is regulated by internal policies and rules, or works agreements. If use is not regulated by the employer, private use is admissible as long as it is kept within reasonable and marginal limits.
Are there any specific requirements for doing so?	As no legislation or law exists regulating private use of the internet, the employee must follow the regulations and policy defined by the employer.
Is the employee allowed to use his/her office e-mail account for private purposes?	As no legislation or law exists regulating the use of office e-mail accounts for private purposes, the legal position is the same as that described in Answer 1, above.
Are there any specific requirements for doing so?	See answer 2, above.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	It depends whether the employer has prohibited private use of an e-mail account or not. If such use is forbidden, then the employer is allowed to check the e-mails. Such checking by the employer raises data protection issues. However, as it is a form of 'processing' under the Austrian Data Protection Act 2000 ("DPA"), the employer must comply with existing 'data protection principles' such as proportionality and legitimate purpose. When it comes to checking the content of an e-mail, the legal consequences depend on the character of the e-mail as either private or business-related. After notifying the employee, the employer may check the content of e-mails relating to business, but not the content of private e-mails. Even if the employer prohibits private use of e-mail accounts, he is not allowed to check the content of e-mails which could be private.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	Yes, because in practice this is likely to make a difference as employees will be entitled to a greater expectation of privacy. If the subject of the e-mail is not appropriate for finding out if the e-mail is related to business or privacy, then the employee must provide information about that. The company is not allowed to check or save the content of an e-mail as soon as it recognises that it has private content, other than in cases involving imminent danger.

Data collection during the application process	
What information is the employer allowed to collect?	Collecting data is covered by the DPA. Consequently, data may only be collected for definite, determined and legitimate purposes. Furthermore, data are only allowed to be used in a way that is compatible with the purpose. In general, the processing of personal data revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of personal data concerning their sex life or health-related personal data, is prohibited.
How long may data of this nature be stored?	The DPA does not prescribe an explicit term for deleting collected data. Pursuant to the DPA, the storage of data is legal as long as it is required to achieve the purpose for which the data is collected. Data collected during an application process has to be anonymised or deleted when the application process has ended. The consent of the person is required for their data to be kept in case of possible future applications.
Is the consent of the employee required?	Yes, the collection of data which is not public or anonymous requires the consent of the employee.
GPS tracking	
Under what conditions can the employer use GPS tracking?	Employee monitoring raises data protection and labour law implications in particular. Implementation of control measures which affect an employee's human dignity is only admissible if a respective works agreement is concluded with the works council. If a works council has not been established, individual agreements with all affected employees are required, or any control measures are unlawful. Basically, the use of GPS tracking is a control mechanism which concerns human dignity. If the use of GPS tracking not only concerns but also infringes human dignity, it is unlawful. So far, the Supreme Court in Austria has no jurisdiction relating to GPS tracking. GPS tracking is also a form of monitoring and collection of personal data. DPA principles therefore have to be observed as described above.
Use of video surveillance	
Is the employer allowed to use video surveillance?	Yes, the employer is allowed to use video surveillance by law (DPA), but only for the purpose of protecting employees or fulfilling legal due diligence. The Austrian Supreme Court has qualified TV cameras installed to monitor employees as affecting human dignity. A respective works agreement, or the consent of each individual employee in the absence of a works council, is therefore necessary.
Are there any specific requirements for doing so?	In general, video surveillance is a control mechanism which affects human dignity, and can only be introduced by entering into a works agreement with the works council. The employer has to report the use of video monitoring to the data security commission. The employer has to sign the video monitoring and record each use of it. The data collected must be deleted within 72 hours.
Are there any situations/ locations where video surveillance is generally prohibited?	Video surveillance is generally prohibited in areas that are completely private, e.g. toilets. Furthermore, video surveillance may not be used for the purpose of controlling the work of employees.

Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	The Supreme Court has not so far reached any legal decisions regarding this issue. The employer may not be allowed to collect such information via social media which he would not be allowed to request in the application process. This relates in particular to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership. The processing of personal data concerning the sex life or health-related personal data of the applicant is also prohibited. Information circulating freely on the internet can be used by the employer. It remains contentious whether information such as that collected via Facebook constitutes 'public' information that can be used by everybody without the consent of the individual involved.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	Yes. See 'Use of internet and e-mail', above.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	The DPA only provides for regulations concerning efficiency controls in connection with video surveillance. Despite the fact that no specific data protection law exists relating to efficiency controls, various forms of controlling and monitoring efficiency do have data protection.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Agreements with works councils may only regulate specific matters reserved for them either by law or by the applicable collective agreements. Various forms of data collection, processing and use may constitute control mechanisms which concern human dignity. In that case, a works agreement must be entered into between the works council and the employer. The principles of the DPA must also be complied with.
To what extent can data collection, processing and use be justified by agreements with unions?	The Labour Constitution Act is the principal source of regulations governing collective bargaining agreements entered into between the trade union and the Austrian Trade Chamber of Commerce. Collective bargaining agreements may only regulate specific matters which are reserved to them by law. As a result, an agreement about data collection, processing and use cannot be entered into.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	One of the ways in which processing can take place is where the employee signifies his or her informed consent to the processing. In cases of sensitive personal data, this consent must be "explicit", i.e. a general consent provision in an employment contract would not suffice.
If so, to what extent?	The consent must comply with the requirements of the definition of 'consent' pursuant to the DPA. Consent must therefore be appropriate to the particular circumstances of the case. Consent obtained under duress does not satisfy the condition for processing. Additionally, there are various formal requirements which have to be fulfilled, i.e. the type size of the declaration of consent may not be smaller than the rest of the text.

Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	Pursuant to the Labour Constitution Act, the employer has to inform the works council about the EDP-supported *('automationsunterstützt')* data he records. He also has to provide information about the way he plans to proceed or transmit data. The works council has the right to check the content of these data.
What kind of participation rights do unions have in relation to data protection?	Trade unions have no rights concerning data protection.
Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	Transfer within a group of companies is a form of processing, and the employer must therefore be able to comply with the principles of the DPA. Data transfer within a group is subject to other, special requirements: the collection and/or processing of data must have complied with the legal prerequisites of the DPA, the recipient must substantiate his authority to receive the data, and the transfer may not infringe the right of nondisclosure of the concerned person.
What are the requirements for data transfer to take place within a group?	See answer above.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	While the transfer of data within the EU is not restricted, the transfer of data to a group company which is located outside the EU requires the approval of the Data Security Commission. The transfer of data to a group company in a third country is permissible without approval if this state guarantees appropriate data protection. The third countries which guarantee appropriate data protection are determined through an order of the Federal Chancellor subject to consideration of the Statements of the European Commission.
Duties of the employer connected with termination of an employment contract	
Are there any duties relating to data protection connected with the termination of an employment contract?	There are no specific duties regulated by law.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	As already mentioned, saving data is only permissible as long as the data involved are required to achieve the purposes for which they were collected. The DPA does not determine a certain point of time for destroying the data.
Contacts	
Contacts within own jurisdiction	Ursula Roberts **E** ursula.roberts@cms-rrh.com
Contacts within jurisdictions different from that mentioned in this list	Johannes Juranek **E** johannes.juranek@cms-rrh.com

Belgium



Group contact: Jef Degrauwe

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	The employer has the right to decide whether employees can freely use the internet or not. The employer has the right to restrict access to the internet and/or control use of the internet subject to certain conditions.
Are there any specific requirements for doing so?	The employee has to follow the regulations set out by the employer.
Is the employee allowed to use his/her office e-mail account for private purposes?	This depends whether regulations relating to this subject have been set out by the employer.
Are there any specific requirements for doing so?	Please see above. This depends whether regulations relating to this subject have been set out by the employer.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	The employer must respect the employee's personal privacy in the workplace. He may, however, monitor the use of e-mail and the internet subject to observance of the relevant legal rules (General Privacy Law of 8 December 1992, and the CBA nr. 81).
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	The employer has the right to exert a limited degree of control in accordance with the employee's privacy and the principles of proportionality, transparency and legitimate purpose.
Data collection during the application process	
What information is the employer allowed to collect?	The processing of personal data is prohibited in principle, unless allowed by the General Privacy Law of 8 December 1992. In general, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of personal data concerning the employee's sex life and health-related personal data, is prohibited.
How long may data of this nature be stored?	No longer than necessary for the purposes for which the data have been collected, or for which they are processed further.
Is the consent of the employee required?	Yes.

GPS tracking	
Under what conditions can the employer use GPS tracking?	There is no legal framework for GPS tracking in Belgium. General privacy principles (proportionality, transparency and legitimate purpose) are applicable.
Use of video surveillance	
Is the employer allowed to use video surveillance?	Yes.
Are there any specific requirements for doing so?	Specific requirements are set out in the CBA nr. 68. Video surveillance is allowed, subject to the principles of transparency, proportionality and legitimate purpose. The General Privacy Law of 8 December 1992 remains applicable to the storage of the data. In the event that not only employees but also other persons (e.g. customers) are filmed, the law of 21 March 2007 on regulation of the installation and the use of surveillance cameras is also applicable.
Are there any situations/ locations where video surveillance is generally prohibited?	No, but video surveillance is only allowed for purposes of health and safety, protection of the goods of the enterprise, control of the production process and control of the work.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	Information circulating freely on the internet can be used by the employer.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	Yes, see 'Use of e-mail and the internet', above.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	No, there is no general legal framework.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Agreements with works councils are possible in theory, but such agreements have to respect the applicable legislation and general privacy principles.
To what extent can data collection, processing and use be justified by agreements with unions?	See answer relating to works councils, immediately above.

Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	In principle, the processing of data requires the consent of the employee. Since the General Privacy Law of 8 December 1992 is compulsory, it cannot be altered by consent of the employee.
If so, to what extent?	Not applicable.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	The General Privacy Law of 8 December 1992 does not provide a specific role for works councils or trade unions. However, more specific regulation of such issues as the use of e-mail and internet do provide information and consultation procedures vis-à-vis works councils and/or trade unions.
What kind of participation rights do unions have in relation to data protection?	See answer relating to works councils, immediately above.
Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	There is no specific regulation in place relating to data transfer within a group. The General Privacy Law of 8 December 1992 provides that personal data may be transferred if the transfer is necessary to achieve an announced and legitimate purpose. The general principles of the General Privacy Law, such as legitimacy, informing data subjects, etc. remain applicable, since transferring data is a form of processing data.
What are the requirements for data transfer to take place within a group?	See answer immediately above.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	Yes. Personal data that are undergoing processing or that are intended for processing after transfer may only be transferred to a country outside the EU if, without prejudice to compliance with the provisions laid down by or by virtue of the General Privacy Law of 8 December 1992, the third country in question ensures an adequate level of protection. Should a company wish to transfer data within its corporate group, including member countries outside the EU, the company can provide Binding Corporate Rules, which have to be adopted by Royal Decree.
Duties of the employer connected with termination of an employment contract	
Are there any duties relating to data protection connected with the termination of an employment contract?	No, there are no specific duties.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	No longer than necessary for the purposes for which the data are collected or for which they are processed further. The General Privacy Law does not foresee an explicit term.

Contacts

Contacts within own jurisdiction	Katarina Magerman **E** katarina.magerman@cms-db.com
Contacts within jurisdictions different from that mentioned in this list	

Bulgaria



Group contact: Maria Drenska, Maya Aleksandrova

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	The law does not prohibit use of the internet at work, other than the employer restricting internet access to certain websites.
Are there any specific requirements for doing so?	There are no specific statutory requirements relating to such use.
Is the employee allowed to use his/her office e-mail account for private purposes?	There are no legal requirements prohibiting the use of office e-mail accounts for private purposes. Nevertheless, the employer may restrict the use of office e-mail accounts solely to the type of usage benefitting the performance of duties under the employment contract.
Are there any specific requirements for doing so?	There are no specific statutory requirements concerning such use, though the employer may establish certain rules regarding the use of office e-mail accounts and provide sanctions when these rules are violated. Such rules may be reflected in the individual employment agreement or the rules on internal order in the enterprise.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	The employer is not prohibited from having access to the employee's office e-mail account. However, the employer may not access the private e-mail account of the employee since the Constitution proclaims the freedom and confidentiality of correspondence which are considered inviolable (the only exception being judicial authorisation in cases where a grave crime has been detected or could be prevented).
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	In cases where the employee uses an office e-mail account for private purposes and the employer has access to it, the employee is strongly advised to set up a separate folder entitled "Personal" for storing data of a purely personal nature.
Data collection during the application process	
What information is the employer allowed to collect?	Generally, this may be any information voluntarily provided by the job applicant. However, the employer is not allowed to collect information related to racial or ethnic origin, political, religious or philosophical convictions, membership of political parties or organisations, associations with religious, philosophical, political or trade union-related objectives, health, sex life or genetic data, except in specific cases.

How long may data of this nature be stored?	The employer may store the personal data until the aims of its collection are realised. The employer is only permitted to store the collected information after its aims are realised as anonymous data for statistical purposes. In such cases, the Bulgarian Personal Data Protection Commission (the "Commission") needs to be notified.
Is the consent of the employee required?	No, as long as he has provided his personal data voluntarily to conclude a (future) employment contract.
GPS tracking	
Under what conditions can the employer use GPS tracking?	Since there are no legal provisions prohibiting GPS tracking, it may be used by the employer if required due to the nature of the work. Otherwise, its use shall be subject to preliminary consent on the part of the employee.
Use of video surveillance	
Is the employer allowed to use video surveillance?	Yes, as long as certain requirements are met.
Are there any specific requirements for doing so?	Before collecting personal information by means of video monitoring, the employer must create a Video Monitoring Register with the Commission. Furthermore, the employer is required to notify its employees of the purposes and duration of the surveillance, as well as of any third parties to whom the information may be disclosed. If third parties are to be subject to video monitoring, the employer is required to set up information boards, informing those third parties of the fact. If the purpose of the video monitoring is control of the labour process, (i) (a legal ground for the monitoring or (ii) explicit consent of the employee is required.
Are there any situations/ locations where video surveillance is generally prohibited?	Video surveillance is generally forbidden under the Bulgarian Constitution. It is only permitted in specific cases, and the person subject to the surveillance must be made aware of the fact.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	There are no restrictions in this regard.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	Yes, see above under 'Use of e-mail and the internet'.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	There are no provisions providing for efficiency controls being carried out on the employee under Bulgarian data protection law.

Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	There are no legal provisions in this regard.
To what extent can data collection, processing and use be justified by agreements with unions?	The law does not prohibit the inclusion of data protection matters in collective labour ageements with unions.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	Yes, in certain cases.
If so, to what extent?	The employer may collect information related to racial or ethnic origin, political, religious or philosophical convictions, membership of political parties or organisations, associations with religious, philosophical, political or tradeunion-related objectives, health, sex life or genetic data if the employee consents to this.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	Works councils have the right to consult the employer when data protection issues are reflected in internal works rules.
What kind of participation rights do unions have in relation to data protection?	Unions should play an active part in drafting all internal rules and regulations in place at the enterprise, including data protection rules.
Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	Yes.
What are the requirements for data transfer to take place within a group?	Upon registration with the Commission, the employer may freely transfer and disclose personal information in any of the 27 Member States of the European Union plus Iceland, Liechtenstein and Norway, after notifying the Commission of the transfer and disclosure of the personal information in the respective country.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	Transferring personal information to a third country (outside the countries above) requires an adequate level of personal data protection within its territory and the parties to the transfer enter into a contract based on the standard contractual clauses approved by the European Commission. In such case the Bulgarian Commission shall be notified for the transfer of data to the third country.
Duties of the employer connected with termination of an employment contract	
Are there any duties relating to data protection connected with the termination of an employment contract?	The Personal Data Protection Act stipulates that personal data shall be stored for as long as required to achieve the purposes of the processing. After this purpose has been achieved (i.e. the employment contract has been terminated), storage is only allowed in cases specifically provided for by law.

How long is an employer allowed/required to keep information concerning an employee who has left the company?	50 years for social security and pensions purposes; other periods may apply in specific cases.

Contacts

Contacts within own jurisdiction	Maria Drenska **E** maria.drenska@cms-rrh.com Maya Aleksandrova **E** maya.aleksandrova@cms-rrh.com
Contacts within jurisdictions different from that mentioned in this list	

Croatia



Group contact: Gregor Famira

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	There is no law preventing employees from accessing the internet at work for private purposes. In some cases, an employer will have policies in place either prohibiting or regulating this access. Such regulation would commonly involve prohibiting use of the internet for commercial or offensive purposes, and limiting time spent using the internet to minimal levels (e.g. during breaks or before/after working time). In order for such policies to be effective and enforceable, they must be brought to the attention of all employees affected in a transparent manner, and must be clear-cut, with no room for misunderstanding.
Are there any specific requirements for doing so?	As explained above, the law does not control employee use of the internet in a work context, but employers normally have policies in place.
Is the employee allowed to use his/her office e-mail account for private purposes?	Again, there is no legislation or other law to prevent an employee from using a work e-mail account for private purposes, but employers can restrict such use through their own policies and rules.
Are there any specific requirements for doing so?	This will depend on the employer's own policies and rules.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	Yes, subject to certain conditions. This raises data protection issues as well as issues relating to privacy of correspondence. As it is a form of 'processing' under the Data Protection Act ("DPA"), the employer will have to comply with the rules relating to the processing of personal data. In principle, it must notify employees that such checking will take place (this is normally set out clearly in the applicable policy) and obtain the employee's approval of the checking. The employer is also required to satisfy a data processing condition, e.g. that the processing is necessary for a legitimate interest of the employer, and to pay attention to issues relating to the use, security and accuracy of the information obtained.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	Yes, as employees will be entitled to a greater expectation of privacy in relation to e-mails that are clearly private, e.g. those marked as "private" or "personal". The employer can still check these e-mails, as long as it complies with the conditions of the DPA (see above).

Data collection during the application process	
What information is the employer allowed to collect?	Collecting data is covered by the DPA. As with any other processing, this means the data subject (i.e. the candidate) must know that this is happening, that the employer must be able to justify the collection, i.e. satisfy at least one processing condition, and that the data collected are: adequate, relevant and not excessive; accurate; kept no longer than needed; processed in accordance with the candidate's rights (this relates principally to the accessing of the data); kept securely; and are not transferred outside Croatia unless adequate protection can be assured in the other jurisdiction (all countries of the European Economic Area are viewed as satisfying this condition). Employers must be careful that they do not collect more information than they actually require, and that the information is only used for the purpose(s) of which the employee has been notified.
How long may data of this nature be stored?	According to the DPA, for no longer than necessary. No opinions of the Croatian Data Protection Agency ("Agency") have been published which specify this provision in greater detail.
Is the consent of the employee required?	Consent is required in principle, as processing a candidate's personal data is usually not justified by law or on other grounds, in which case consent would not be required.
GPS tracking	
Under what conditions can the employer use GPS tracking?	According to an opinion issued by the Agency in 2008, the principle of installing GPS devices for official business purposes only is not contrary to the principles of the DPA. Collection of data is subject to observance of DPA rules.
Use of video surveillance	
Is the employer allowed to use video surveillance?	In principle, this is permissible.
Are there any specific requirements for doing so?	In addition to normal DPA principles, all workers (and any third persons) should normally be aware of its use. Covert monitoring can be justified as part of a specific investigation, e.g. where criminal activity is suspected and the use will be limited.
Are there any situations/ locations where video surveillance is generally prohibited?	No specific rules are in place regarding this. However, based on the principle that the employee's privacy should be protected, surveillance should not take place in areas workers would expect to be private, such as toilet areas or private offices.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	Employers can use social media as a source of information. However, information obtained via social media should not result in discrimination between applicants (on grounds specified by law, such as family status, sexual orientation, political orientation, etc.).
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	It is possible for an employer to regulate this by having an appropriate policy in place. This policy must be justified on business-related grounds, however, and neither excessive nor burdensome upon employees in its nature. In the absence of a clear policy, it is very difficult to regulate the content of social media.

Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	There is no specific data protection law relating to efficiency controls, but various forms of controlling and monitoring efficiency will have data protection implications.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Any data processing (including collection and use) must be justified by reference to one or more of the processing conditions set out in the DPA (and one or more sensitive processing conditions in the case of sensitive personal data). An agreement with a works council that processing is reasonable or required, etc. may be helpful evidence supporting the employer's given justification, but is not enough in itself to permit the processing of personal data.
To what extent can data collection, processing and use be justified by agreements with unions?	Data protection issues are usually not subject to agreement between employers and unions in Croatia, but between employers and works council instead. If a works council does not exist, however, but a trade union is active at the company, then the same rules apply to such a representative body, and the same limits on justification apply as mentioned above.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	One of the ways in which processing can take place is when the data subject (the employee, in this case) signifies his or her informed consent to the processing. This consent must be "explicit" in the sense that the employee has to consent to the collection of specifically identified data; a reference to data in general would not suffice. Even with such consent, however, the employer must not deviate from other data processing rules contained in the DPA.
If so, to what extent?	See answer above. Referring generally to the consent issue, it should be noted that consent must be appropriate to the particular circumstances of the case. Additionally, consent obtained under duress will not satisfy the condition for processing. Where 'sensitive personal data' (race/ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical/mental health, sex life or criminal record) is to be processed, an additional processing condition must be satisfied from a separate list in the DPA, and explicit consent is often required for this purpose.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	The employer must obtain prior approval from the works council before reaching any decision relating to the collection, processing, use or delivery to third persons of employees' personal data. The same applies to a decision affecting the appointment of a person who will be in charge of the supervisions of the treatment of the employees' personal data within the company (only obligatory for an employer employing 20 and more employees).
What kind of participation rights do unions have in relation to data protection?	No automatic rights. If a works council does not exist, however, but a trade union is active at the company, then the same rules apply to such a representative body, and the same comment as above applies.
Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	There is no specific regulation on this point. It is clear, however, that information given to employees about any processing should make clear how that information is to be used and shared, and whether it is to be shared with other group companies.

What are the requirements for data transfer to take place within a group?	Transferring data to a group company is a form of processing, so the employer must comply with the normal DPA requirements, including being able to satisfy a processing condition (and a sensitive data processing condition if applicable).
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	Yes. Where data are to be transferred to a country within the European Economic Area, no prior opinion of the Agency is required, and no further conditions need be met before the transfer (besides following basic DPA rules). If the data are being transferred outside the EEA, the opinion of the Agency needs to be obtained prior to the transfer on whether the respective country can ensure the personal data will be adequately protected. If the Agency states that this is not the case, then additional conditions must be met for the transfer to be allowed.

Duties of the employer connected with termination of an employment contract

Are there any duties relating to data protection connected with the termination of an employment contract?	No particular duties. Termination of the employment relationship may only raise the question of whether the employer may continue to hold and process personal data, and for how long.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	Businesses must ensure they do not retain the personal data of former employees once there is no longer a legitimate business need or legal requirement to do so. There is no specific timescale in the DPA, as it is recognised that there a number of different reasons and circumstances could apply.

Contacts

Contacts within own jurisdiction	Gregor Famira **E** gregor.famira@cms-rrh.com
Contacts within jurisdictions different from that mentioned in this list	

Czech Republic



Group contact: Tomáš Matějovský, Jakub Tomšej

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	It is up to the employer to decide whether its employees can use, for private purposes, an internet connection provided by the employer. The internet can therefore be used by employees for private purposes provided that the employer specifically allows it.
Are there any specific requirements for doing so?	The internet can be used by employees for private purposes if this is specifically allowed by the employer.
Is the employee allowed to use his/her office e-mail account for private purposes?	It is up to the employer to decide whether an employee can use, for private purposes, the employee's office e-mail account provided by the employer. The employee's office e-mail account provided for the employee by the employer can therefore be used by the employee for private purposes if this is specifically allowed by the employer.
Are there any specific requirements for doing so?	An employee's office e-mail account provided for the employee by the employer can be used by the employee for private purposes if this is specifically allowed by the employer.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	In general, an employer is only entitled to check e-mail messages that can be considered to be business correspondence of the employee entered into on behalf of the employer. Consequently, an employer is not entitled to check any private e-mail communication of the employee, even if such private e-mail communication was entered into by the employee using the office e-mail account provided by the employer. If the employer wishes to check an employee's e-mails containing business correspondence, the following conditions must be fulfilled: (i) there must be a specific serious reason consisting of the employer's activities of a special nature, which justifies such monitoring of e-mails by the employer; and (ii) employees must be informed in advance of the scope and manner of performance of the e-mail monitoring.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	As described in the previous answer, an employer is only entitled to check e-mail messages (subject to the conditions specified in the previous answer) that can be considered business correspondence of the employee on behalf of the employer. Consequently, an employer is not entitled to check any private e-mail communication of the employee, even if such private e-mail communication has been entered into by the employee using the office e-mail account provided by the employer.

Data collection during the application process	
What information is the employer allowed to collect?	An employer is only entitled to collect information directly connected with the performance of work and the employment relationship. Certain types of information can only be collected if relevant to specific types of work the employee performs (e.g. pregnancy, family affairs, criminal record), whilst certain information (e.g. sexual orientation, membership of trade unions and political parties, religion) must never be collected.
How long may data of this nature be stored?	No express time limit is stipulated under Czech law. In practice, however, it is acceptable to store data during the term of employment as well as during the limitation period during which employment- related claims can be raised after termination of the employment. The general limitation period for employment related claims is three years, although in some specific cases (e.g. data concerning statutory health insurance, etc.) longer periods are prescribed by law.
Is the consent of the employee required?	No, if an employer only collects such personal data as it is specifically authorised to do by law (the employee's name, surname, etc.). If the employer wishes to collect other types of personal data of an employee (such as that employee's private e-mail address, etc.), then it must gain the employee's specific consent to the data being collected.
GPS tracking	
Under what conditions can the employer use GPS tracking?	There is no specific law regulating the use of GPS tracking in an employment relationship, and in practice, monitoring employees in this way could raise many controversies and different legal opinions. In general, however, GPS tracking is not expressly forbidden in an employment relationship and, in our view, it could be used if the following two main conditions are fulfilled: (i) there must be a specific serious reason consisting of the employer's activities of a special nature, which justifies such monitoring by the employer; and (ii) employees must be informed in advance of the scope and manner of performance of the monitoring.
Use of video surveillance	
Is the employer allowed to use video surveillance?	Yes, but only if the following two main conditions are fulfilled: (i) there must be a specific serious reason consisting of the employer's activities of a special nature, which justifies such monitoring by the employer; and (ii) employees must be informed in advance of the scope and manner of performance of the monitoring.
Are there any specific requirements for doing so?	Yes, but (i) there must be a specific serious reason consisting of the employer's activities of a special nature, which justifies such monitoring by the employer; and (ii) employees must be informed in advance of the scope and manner of performance of the monitoring.
Are there any situations/ locations where video surveillance is generally prohibited?	No specific locations/situations are expressly excluded by Czech law. In general, however, the video surveillance should not involve inappropriate interference with the employee's privacy. In practice, therefore, it is understood that video surveillance should not be used in places such as bathrooms, changing rooms, etc.

Social media

Is the employer allowed to use social media as a source of information concerning a job applicant?	This issue is controversial under Czech law, and different opinions have been expressed. In our view, however, it is generally possible to use social media as a source of information as long as the following conditions are fulfilled: (i) that the social media profile of an employee is publicly available; (ii) that the employer could use only such data relevant to the purpose in question, i.e. the negotiation of an employment agreement (on this basis, the employer would not be able to use the following types of information obtained from social media: racial origin, sexual orientation, pregnancy, membership of trade unions or political parties, family and property affairs, religious denomination, etc.); and (iii) that personal data obtained from social media is stored for a limited time only, generally during the time an employment contract is being negotiated.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	In general, an employer is allowed to prescribe rules to regulate use of social media by employees provided the employees access the social media via equipment provided by the employer, i.e. a computer and internet connection provided by the employer. As far as content is concerned, employees must not use social media to disclose information which makes up part of the employer´s confidential commercial information, or where they are bound by a statutory or contractual duty to maintain confidentiality.

Efficiency control

Does data protection law provide for any regulations relating to controls on the efficiency of employees?	Czech data protection law does not include any special rules on efficiency controls of employees. However, various forms of efficiency controlling and monitoring could have data protection implications.

Justification of data collection, processing and use with the help of the works council/unions

To what extent can data collection, processing and use be justified by agreements with works councils?	An agreement with works councils regarding personal data processing might be helpful to show the employer cares for its employees´ personal data. From a strictly legal point of view, however, such an agreement regarding data processing with works councils would not be sufficient to actually permit the processing of personal data of employees.
To what extent can data collection, processing and use be justified by agreements with unions?	An agreement with trade unions regarding personal data processing might be helpful in order to show the employer cares for its employees´ personal data. From a strictly legal point of view, however, such an agreement regarding data processing with trade unions would not be sufficient to actually permit the processing of employees' personal data.

Justification by consent of the employee

Can the regulations of data protection law be altered by consent of the employee?	In general yes, if it is in favour of the employee. In most cases, consent from an employee can enable the employer to collect a wider scope of the employee´s data than it would be entitled to collect without the employee´s consent directly based on the relevant laws alone.
If so, to what extent?	In most cases, consent from an employee can enable the employer to collect a wider scope of the employee´s data than it would be entitled to collect without the employee´s consent directly based on the relevant laws alone.

Participation rights of the works council and unions

What kind of participation rights do works councils have relating to data protection?	No specific rights.

What kind of participation rights do unions have in relation to data protection?	The employer is obliged to consult trade unions regarding all measures affecting larger numbers of employees (including measures concerning data protection).

Data transfer within a group

Does data protection law provide for any special regulations relating to data transfer within a group?	No.
What are the requirements for data transfer to take place within a group?	General rules for data transfer would apply (such as concluding a data processing agreement between the data controller and data processor, etc.). Czech law does not have any special rules that would give companies within one group more lenient conditions for data transfer within the group than in the case of companies transferring data outside their group.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	No, general rules for data transfer outside the EU would apply. Czech law does not have any special rules that would give companies within one group some more lenient conditions for data transfer within the group than in the case of companies transferring data outside their group.

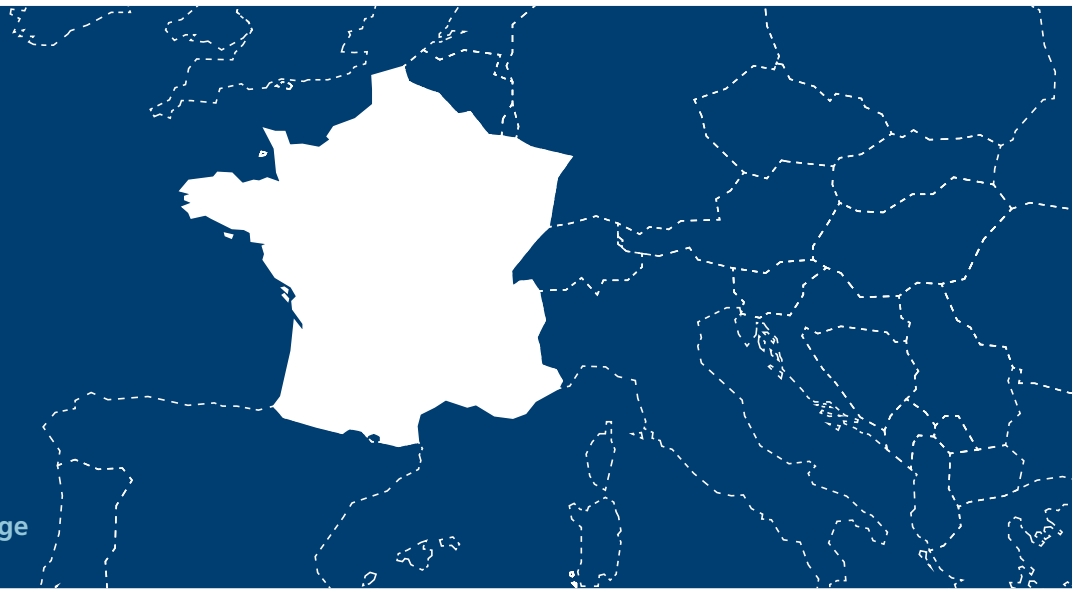
Duties of the employer connected with termination of an employment contract

Are there any duties relating to data protection connected with the termination of an employment contract?	The employer would have to consider how long it can continue to keep and process the personal data of the employee.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	No express time limit is stipulated by Czech law. In practice, however, it is acceptable to store the data during the limitation period during which employment-related claims can be raised after the employment has been terminated. The general limitation period for employment-related claims is three years, although in some specific cases (e.g. where data concerning statutory health insurance, etc. is involved) longer periods may be prescribed by law.

Contacts

Contacts within own jurisdiction	Tomas Matejovsky **E** tomas.matejovsky@cms-cmck.com Jakub Tomšej **E** jakub.tomsej@cms-cmck.com
Contacts within jurisdictions different from that mentioned in this list	

France



Group contact: Vincent Delage

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	It is common for employers to have a policy in place that either prohibits or regulates use of the internet. Moreover, according to Article L. 1121–1 of the French Labour Code, an employer cannot restrict his employees' rights and individual liberties if it is not strictly justified by the nature of the employees' duties and proportionate to the purposes of such restrictions. Any provision taken in violation of this fundamental principle is prohibited. As a consequence the use for personal and limited access would be allowed by the French Supreme Court.
Are there any specific requirements for doing so?	If the employer would like to set up rules relating to use of the internet by employees, it should first consult the works council and inform the employees of the rules set up. As a consequence of the rule described above, the employer could only state that use of the internet by the employee for personal purposes must not be excessive.
Is the employee allowed to use his/her office e-mail account for private purposes?	In principle, no. But here again, the principle cited in the point above makes it difficult to prohibit use entirely, and short and limited use would be allowed by the judge.
Are there any specific requirements for doing so?	Please see the answer above.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	The employer must respect the employee's personal privacy in the workplace. It cannot check the employee's e-mails if they are indicated as being "private" or "personal". There can be no exception to this rule. The employer should first consult the works council and inform employees of any rules set up concerning the checking of professional e-mails.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	Not applicable.
Data collection during the application process	
What information is the employer allowed to collect?	The employer may only collect the information related to the applicant's capacity to do the job. The following information about the candidate could be considered as valid: their first name (names); surname; date of birth; residential address (address for correspondence); and education and employment history.

How long may data of this nature be stored?	For candidates for a job who have not been employed by the company, the said company can keep the personal data for a maximum period of two years after the last contact with the candidate.
Is the consent of the employee required?	According to the Labour Code, personal information relating to an individual cannot be collected using a method that has not been formerly disclosed to the individual in question. French law provides for a right to object that any individual can freely exercise at any time from the data collection onwards, e.g. by requesting that data contained in commercial data files be removed. This right only applies to processing that is not mandatory by law (e.g. an employer has an obligation to keep certain information on his or her employees for tax and social security purposes). The treatment of such information is subject to a specific declaration to a public office, the CNIL. Generally, consent is required before processing personal information. Consent must be explicit, unambiguous, freely given, specific and informed. Consent must be specific with regard to a clearly identified processing operation, and documented in writing. Consent is also required if: 1. Personal information is to be processed for a purpose other than that previously authorised by the individual (Secondary Use); 2. Personal information from the EU is transferred to a country outside the EU which is not recognised by the EU as offering adequate protection, and the transfer is not legitimised by another legal mechanism; 3. Sensitive information is processed. Exceptions to consent requirements include: 3.1. Processing necessary for the subject of the data to perform a contract; 3.2. Processing necessary for the data controller to meet a legal obligation (e.g. for the employer to to meet its statutory duties); 3.3. Processing to protect the vital interests of the data subject; 3.4. Processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or 3.5. Processing necessary for the purposes of the legitimate interests of the controller, except where such interests are overridden by the interests of the fundamental rights and freedoms of the data subject.
GPS tracking	
Under what conditions can the employer use GPS tracking?	According to Article L. 1121–1 of the French Labour Code, an employer cannot restrict his employees' rights and individual liberties if this is not strictly justified by the nature of the employees' duties and proportionate to the purposes of such restrictions. Moreover, the implementation of a GPS tracking system should not lead to the permanent control of the employees, it should not allow the employer to gain access to data concerning excess speed information, it should be accompanied by measures ensuring safe access to the information, and it cannot concern the staff representatives in the context of their mandate. The right of an employer to monitor his employees' activity is subject to prior consultation with the employees' representatives (works councils and the Hygiene and Safety Committee), and prior information of each employee involved. It should be limited to cases involving security matters and better delivery of goods.
Use of video surveillance	
Is the employer allowed to use video surveillance?	Yes, but only if strictly necessary.

Are there any specific requirements for doing so?	Use of video surveillance in a place which is not accessible to the public (such as a stockroom) is subject to the CNIL being notified of that use.Specific and strict formalities are applicable to the use of a video surveillance system in a place accessible to the public. Moreover, the company must inform the public and employees, and consult the works council, the Hygiene and Safety Committee and visitors of the following: the existence of the system; the identity of the company; the recipients of the recordings; and the practical details of the access to the recordings. Moreover, any individual whose image is recorded should be able to have access to the recordings. The recordings should be viewed by authorised people in the framework of their functions (their names/functions will have to be mentioned in the notification to the CNIL of the request for authorisation to the Prefect). The Act of 21 January 1995 mentions that the duration is set by the prefectural authorisation but provides that the storage should not last more than one month (Article 10 IV of the Act nr. 95–73 of 21 January 1995). In all cases, the right of an employer to monitor his employees' activity is subject to a prior consultation with the employees' representatives (works councils and the Hygiene and Safety Committee), and the prior notification of all employees involved.
Are there any situations/ locations where video surveillance is generally prohibited?	According to Article L. 1121–1 of the French Labour Code, an employer cannot restrict his employees' rights and individual liberties if this is not strictly justified by the nature of the employees' duties and proportionate to the purposes of such restrictions. In practice, therefore, it is understood that video surveillance should not be placed in places such as bathrooms, changing rooms, etc., or in offices where there is no specific risk of theft.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	Information circulating freely on the internet can be used by the employer unless it is not needed to protect his legitimate interests. An employer would not be allowed to use social media to look into the sexual preferences or politic opinions of an employee, for example.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	Yes, see 'Use of internet and e-mail', above.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	The right of an employer to monitor his employees' activity is subject to a prior consultation with employee representative bodies (works councils and the Hygiene and Safety Committee), and prior notification of all employees involved. Use of such a system is also subject to the CNIL being notified.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Such agreements must be more favourable for employees than if there were no agreement in place.
To what extent can data collection, processing and use be justified by agreements with unions?	Such agreements must be more favourable for employees than if there were no agreement in place.

Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	No.
If so, to what extent?	Not applicable.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	The right of an employer to monitor his employees' activity (internet, e-mails or social media) is subject to a prior consultation with employees' representative bodies (works councils and the Hygiene and Safety Committee), but there is no veto right. Employees must also be informed prior to any such controls being used.
What kind of participation rights do unions have in relation to data protection?	None, except by signing agreements enlarging employees' rights.
Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	Data transfer within a group is not regulated in any different way than regular data transfer between an employer and a third party. In the event of such a transfer, all legal requirements must be fulfilled, without exception. Please see below.
What are the requirements for data transfer to take place within a group?	Please see below.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	The transfer of personal data to a country located outside the EEA (Economic European Area) is prohibited, unless the country offers an "adequate level of protection". A country will be considered as offering an adequate level of protection if: (i) where the beneficiary is located in the US, the beneficiary is a member of the Safe Harbor Program; (ii) the country is regarded as offering an adequate level of protection by the European Commission; (iii) the parties to the transfer enter into a contract based on the standard contractual clauses approved by the European Commission; (iv) where the transfer occurs within a group of companies, the group has adopted Binding Corporate Rules (which only apply to multinational organisations transferring personal information outside the EEA but within their group of companies). Other formalities should be fulfilled with the CNIL.
Duties of the employer connected with termination of an employment contract	
Are there any duties relating to data protection connected with the termination of an employment contract?	Personal data can be kept by the employer during the term of the employment contract. The employer can, however, archive the documents in accordance with CNIL requirements. The employer can use non-personal information (e-mails, surfing) to justify dismissal proceedings as long as it respects all the requirements (CNIL declaration, works council consultation, and employee notification).
How long is an employer allowed/required to keep information concerning an employee who has left the company?	The data can be kept as long as the employment contract is being performed, but can also be kept in the form of archives. In the latter case, the data must be stored for a specific period of time, which will depend on the kind of archive, in accordance with the recommendation of the CNIL relating to the archives. In the event of litigation, it can be useful if the employer has kept information about its former employee.

Contacts

Contacts within own jurisdiction

Alain Herrmann
E alain.herrmann@cms-bfl.com
Vincent Delage
E vincent.delage@cms-bfl.com
Anne Laure Villedieu
E anne-laure.villedieu@cms-bfl.com

Contacts within jurisdictions different from that mentioned in this list

Germany



Group contact: Carsten Domke, Bernd Roock, Christopher Jordan

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	Without the permission of the employer, the employee is not allowed to use the internet for private purposes. The employer has the right to decide whether private use of the internet is allowed or not. Use is usually regulated by internal policies and rules, or works agreements. Company practice of tolerating private use without adequate regulation or even contrary to corresponding control can give the employee the right to use the internet for private purposes.
Are there any specific requirements for doing so?	As there is no law regulating private use of the internet, the employee must follow the regulations and policies provided by the employer. When setting up rules relating to use of the internet by employees, the employer needs to respect the works councils' codetermination rights (Section 87 (1), Nos. 1 and 6 of the German Works Constitution Act ("BetrVG").
Is the employee allowed to use his/her office e-mail account for private purposes?	As there is no law regulating the use of business e-mail accounts for private purposes, see answer regarding the internet.
Are there any specific requirements for doing so?	See answer regarding the internet.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	The employer is only allowed to check the employee's e-mails within the scope of Section 32 of the German Federal Data Protection Act ("BDSG"). As a rule, but subject to company circumstances, business e-mails may be checked and read, but private e-mails may not be. The admissibility of data collection depends on the necessity of the implementation, the completion or settlement of the employment relationship. The employer has to pursue a justifiable interest which is higher than the employee's interest when checking the employee's e-mails. In principle, it is recommended that the employee has to be informed in advance.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	Yes. Depending on whether private use is allowed or not, the employer has to consider different standards. Restrictions on checking employee's e-mails are lower with respect to data protection law if private use is prohibited. By allowing private use of e-mail in the workplace, the employer risks being qualified as a telecommunications service provider, such admissibility of control is restricted according to Section 88 of the German Tele-communications Act ("TKG") (controversial).

Data collection during the application process	
What information is the employer allowed to collect?	The employer may collect data as long as it has a legitimate interest (legitimate business need) in terms of the employment relationship.
How long may data of this nature be stored?	The BDSG does not contain an explicit term for deleting collected data. Pursuant to the BDSG, the storage of data is legal as long as it is required to achieve the purpose for which the data is collected. If an employment relationship is not established, then the data must be deleted unless the applicants have agreed to the additional storage.
Is the consent of the employee required?	According to the BDSG, data can be collected without the consent of the employee, subject to the provisions of Section 32, BDSG.
GPS tracking	
Under what conditions can the employer use GPS tracking?	There is no specific rule relating to GPS tracking in Germany. For this reason, the general privacy principles of Section 32, BDSG are applicable. Its admissibility depends on the necessity for the implementation, completion or settlement of the employment relationship. The employer has to pursue justifiable interests which are higher than the employee's interests.
Use of video surveillance	
Is the employer allowed to use video surveillance?	Yes.
Are there any specific requirements for doing so?	Video surveillance is permitted under the general rule of Section 32, BDSG. Accordingly, video surveillance can only be admitted if the employer pursues a justifiable interest (e. g. protection of the employer's property, reasonable suspicion of violations of the employer's or employee's rights, taking into consideration the duration of the surveillance and excluding employees' essentially private spheres). The employer's interest must outweigh the employee's legitimate interest in not being permanently monitored (general personality right).
Are there any situations/ locations where video surveillance is generally prohibited?	There is no general prohibition. However, monitoring of premises which mainly serve the private sphere (toilet, changing rooms) is regularly void due to the balancing of interests.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	In principle, data must be collected directly from the employee. If the employer has informed the employee prior to the survey, the employer must collect data that are generally available without the involvement of the employee as long as employees' legitimate interests do not outweigh this. With regard to data from social networks, serving electronic communication and being password-protected, the legitimate interests of employees outweigh those of the employer. Information from a social network which is used for the presentation of professional qualifications can be used by the employer.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	Concerning the scope for using social media, see 'Use of e-mail and the internet', above. Concerning content on social media, employees must not disclose information which comes under the employer's business secrets or where they are bound by a statutory or contractual duty to maintain confidentiality. Apart from that, the employer cannot influence the use of social media (in terms of content or scope) for private purposes after work.

Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	German Data Protection Law does not contain a specific rule on efficiency controls of employees. Efficiency controls are therefore permitted under the general rule of Section 32, BDSG. The admissibility of data collection depends on the necessity for the implementation, completion or settlement of the employment relationship. The employer must pursue justifiable interests which are higher than the employee's interests, and such control must be a proportionate means of pursuing such interests. In principle, the employer has a legitimate need for information on its employees. However, the works council's rights to codetermination must be observed.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Agreements with the works council may justify the collection, processing and use of data. The agreements have to respect the general privacy principles, but can deviate from legislation (BDSG).
To what extent can data collection, processing and use be justified by agreements with unions?	Same principle applies as for the works council, above.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	In principle, the employee can give his consent to the processing of his personal data. The consent has to be voluntary and in written form. In cases of sensitive personal data, this consent must be "explicit", so that a general consent provision in an employment contract would not suffice. However, legal scholars are controversially discussing whether and under what conditions employees' consent to data processing can be deemed "voluntary".
If so, to what extent?	Please see the answer above.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	The works council is responsible for ensuring the implementation of employee protection laws, such as the BDSG (Section 80 I, nr. 1 of the Works Constitution Act). The employer has to inform the works council about personal data processing activities. As well as this, many other rights of works councils must be observed, such as the right of participation in the implementation of surveillance systems (Section 87 I, nr. 6 of the Works Constitution Act), the right of participation in the general rules of conduct or regulations in operation (Section 87 I, nr. 1 of the Works Constitution Act) and the right of participation in staff questionnaires and personnel evaluation systems (Section 94 of the Works Constitution Act).
What kind of participation rights do unions have in relation to data protection?	Unions do not have specific rights.
Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	The BDSG does not include a provision on corporate matters. Group companies are therefore treated in the same way as third parties.

What are the requirements for data transfer to take place within a group?	Data transfer within a group requires special justification: (i) by formal order data processing agreement; (ii) by works agreement; (iii) by employee's consent; (iv) by specific needs of the employment relationship.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	Yes. Transferring personal data to a country located outside the EU and EEA (Economic European Area) is prohibited unless the country offers an "adequate level of protection". A country will be considered as offering an adequate level of protection if: (i) where the beneficiary is located in the US, the beneficiary is a member of the Safe Harbor Program; (ii) the country is regarded as offering an adequate level of protection by the European Commission; (iii) the parties to the transfer enter into a contract based on the standard contractual clauses approved by the European Commission; (iv) where the transfer occurs within a group of companies, the group has adopted Binding Corporate Rules.

Duties of the employer connected with termination of an employment contract

Are there any duties relating to data protection connected with the termination of an employment contract?	There are no special duties. Termination of the employment relationship only raises the question of whether the employer may continue to hold and process personal data and for how long. According to the BDSG, the employer is only allowed to utilise employees' personal data if use of the respective data is necessary for the employment relationship to be terminated.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	The BDSG prescribes no explicit term for deleting collected data. Pursuant to the BDSG, the storage of data is legal as long as it is required to achieve the purpose for which the data is collected, or if other justified interests exist.

Contacts

Contacts within own jurisdiction	Björn Gaul **E** bjoern.gaul@cms-hs.com Achim Lindemann **E** achim.lindemann@cms-hs.com Michael Kamps **E** michael.kamps@cms-hs.com Christian Runte **E** christian.runte@cms-hs.com Andrea Bonanni **E** andrea.bonanni@cms-hs.com Carsten Domke **E** carsten.domke@cms-hs.com
Contacts within jurisdictions different from that mentioned in this list	

Hungary



Group contact: Gabriella Ormai

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	Similarly to the UK, there is no law preventing employees from accessing the internet at work for private purposes, but it is very common for an employer to have a policy in place that either prohibits or regulates this. Such regulation would commonly involve prohibiting use of the internet for commercial or offensive purposes, and limiting the amount of time spent using the internet to minimal levels (e.g. during breaks or before/after working time).
Are there any specific requirements for doing so?	As explained above, the law does not control employee use of the internet in a work context, but employers normally do.
Is the employee allowed to use his/her office e-mail account for private purposes?	Similarly to the UK, there is no legislation or other law that prevents an employee using a work e-mail account for private purposes, but employers will typically control this through their own policies and rules.
Are there any specific requirements for doing so?	This will depend on the employer's own policies and rules.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	As a general rule, employers shall be allowed to monitor (record) the conduct of employees but only to an extent pertaining to the employment relationship. The employer's actions of control, and the means and methods used, shall not infringe human dignity. The employees shall receive preliminary information on the means and methods used. The employee shall also be informed in advance that the e-mail can be used only for business purposes and other details of the data processing e.g. the scope of the data being processed, the purpose of the data processing, the entity which will control/process the data, the person(s) to whom the data may be disclosed, the duration until such data will be processed, if there is any data transfer outside the European Economic Community, the relevant rights and remedies, and whether consent is mandatory or voluntary. This kind of information is usually provided in a staff handbook, or the employment contract. The employees shall accept in writing the receipt of the staff handbook or accept its provisions as binding on themselves. This would preclude any subsequent disputes over whether employees have received adequate information on the monitoring. According to the Hungarian Information Commissioner, the prior consent of both the sender and the receiver is required for the monitoring. This may be impossible to comply with in practice, and there is no publicly available case where the Information Commissioner has imposed sanctions in connection with the monitoring of an external communication where the above rules have been complied with. In practice, it is customary for the footer of e-mails sent by employees to contain a notification

	on behalf of the employer company (besides other information, e.g. the confidential nature of the e-mail, actions to be taken if the e-mail is received by mistake, opt-out possibilities, etc.) stating that the contents of the e-mail may be monitored by the sender's employer company for security purposes.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	This is likely to make a difference in practice, as employees will be entitled to a greater expectation of privacy in relation to e-mails that are clearly private, e.g. that are marked as "private" or "personal". In theory, however, the employer can still check these e-mails if the employees are informed thereof (as outlined above). According to the Information Commissioner, the employer shall do its best to separate private e-mails from business e-mails in the course of the monitoring.
Data collection during the application process	
What information is the employer allowed to collect?	An employee may only be requested to make a statement or to disclose certain information if this does not violate his/her personal rights, and it is deemed necessary for the conclusion, fulfilment or termination of the employment relationship. An employee may be requested to take an aptitude test if this is required by employment regulations, or deemed necessary with a view to exercising rights and fulfilling obligations in accordance with employment regulations. Note: examples of such aptitude tests shall include, amongst others, a pregnancy test or a certificate thereof. According to the Information Commissioner, questions regarding the financial status, housing conditions or personal data of close relatives may be deemed as a violation of the applicant's personal rights.
How long may data of this nature be stored?	There is no law expressly regulating this issue. It is advisable to keep documents in connection with an application/interview in the event that a legal dispute arises regarding the application (e.g. the applicant may allege that his/her application was refused on the basis of discrimination). The recommended retention period is three to five years.
Is the consent of the employee required?	The applicant shall be informed of the retention of the personal data collected during the application, and shall consent to it. In addition, he/she shall be informed of the details of the processing of his/her personal data.
GPS tracking	
Under what conditions can the employer use GPS tracking?	There is no law expressly regulating this specific issue. As a general rule, employers shall be allowed to monitor (record) the conduct of the employees but only to an extent pertaining to the employment relationship. The employer's actions of control, and the means and methods used, shall not infringe human dignity. The employees shall receive preliminary information on the means and methods used. The employee shall also be preliminarily informed of other details of the data processing, e.g. the scope of the data processed, the purpose of the data processing, the entity which will control/process the data, the person(s) to whom the data may be disclosed, the duration until such data will be processed, if there is any data transfer outside the European Economic Community, the relevant rights and remedies, and whether consent is mandatory or voluntary. This kind of information is usually provided in a staff handbook, or the employment contract. The employees shall accept in writing the receipt of the staff handbook or accept its provisions as binding on themselves. This would preclude any subsequent disputes over whether employees have received adequate information on the monitoring. According to the Information Commissioner, GPS tracking, in company cars, for example, is allowed only if absolutely necessary to monitor the use of the relevant equipment in working hours. The employee shall be able to turn the GPS off where the equipment is used privately (e.g. when on holiday or outside working hours).

Use of video surveillance	
Is the employer allowed to use video surveillance?	According to the Information Commissioner, the installation of CCTV which records the employee's activities is also subject to the advance consent of the employees. In practice, such consent may be given by "implied conduct", i.e. the employer shall install a sign notifying the employees of the monitoring, and the employees implicitly consent to such data processing by entering the premises. Nevertheless, the installation of CCTV is only allowed if the relevant purposes are significant and cannot be achieved by other methods.
Are there any specific requirements for doing so?	The employee shall post a warning or information sign in a clearly visible place, written in an easily understandable fashion to convey useful information to third persons seeking admission onto the property and including the following: the use of the CCTV, its purpose, the place where recordings are stored and period of storage, the person using (operating) the system, the persons authorised to access these data, and the rights of data subjects and procedures for enforcing such rights. The operation of CCTV shall be registered at the Information Commissioner if it also records the movements of non-employees or is operated by an external service provider.
Are there any situations/ locations where video surveillance is generally prohibited?	CCTV shall not be used in a place where surveillance is likely to violate human dignity, such as in dressing rooms, fitting rooms, washrooms, toilets, showers or social areas. It is not permitted to install CCTV in premises where continuous work takes place, e.g. in offices or factories, except where the health of the employee may be in clear and present danger, e.g. on industrial premises or where other hazardous work is done.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	Similarly to the UK, employers can use social media as a source of information. This approach can create legal issues, however: if an employer appears to base its recruitment decisions on (sensitive) personal information found on a social media site, for example, this could lead to a discrimination claim.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	Similarly to the UK, it is possible for an employer to regulate this by having an appropriate policy in place, and this is very much recommended. The absence of a clear policy can make it very difficult to regulate social media.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	There is no specific data protection law relating to efficiency controls, but various forms of controlling and monitoring efficiency will have data protection implications. As a general rule, if there is any personal data processing as part of the efficiency control, then the prior consent of the employee is required. The data processing shall be adequate, relevant and not excessive in relation to the employment purposes.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Similarly to the UK, any data processing (including collection and use) must be justified by reference to one or more of the processing conditions in the Hungarian Data Protection Act (Act CXII of 2011). Agreement with a works council that processing is reasonable or required, etc. may be helpful evidence in supporting the employer's given justification, but is not enough in itself to permit the processing of personal data.

To what extent can data collection, processing and use be justified by agreements with unions?	Similarly to the UK, any data processing (including collection and use) must be justified by reference to one or more of the processing conditions in the Hungarian Data Protection Act. Agreement with a trade union that processing is reasonable or required, etc. may be helpful evidence in supporting the employer's given justification, but is not enough in itself to permit the processing of personal data.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	No. The provisions of the data privacy laws are mandatory, and the parties cannot alter them, even upon mutual consent.
If so, to what extent?	Similarly to the UK, consent must be appropriate to the particular circumstances of the case. Additionally, consent obtained under duress may not satisfy the condition for processing. Only those personal data can be processed which are not excessive and are eligible for the purpose of the processing (employment), and only to the extent and until such time as the data are required for the relevant purpose. This is particularly applicable to sensitive personal data.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	Employers shall consult the works council (if any exists) at least 15 days prior to adopting a decision in connection with, *inter alia,* plans for actions or internal regulations affecting a large number of employees (substantive interest), amongst others, and affecting the processing and protection of the employee's personal data.
What kind of participation rights do unions have in relation to data protection?	Unions do not have such participation rights; they are entitled to request information on data processing at any time, however.
Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	Similarly to the UK, there is no specific regulation on this point. It is clear, however, that information given to employees about any processing should define how that information is to be used and shared, which includes explaining if it will be shared with group companies. Each group company is treated as a separate entity (data controller/data processor) under Hungarian law.
What are the requirements for data transfer to take place within a group?	Transfer to a group company is a form of processing, so the employer must be able to comply with the normal requirements of the Hungarian Data Protection Act, including being able to satisfy a processing condition.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	Yes. Data processors may transfer personal data to data processors that process data in third countries – countries outside the European Union/European Economic Area ("EEA") – or technical data processors that technically process data in a third country if (a) it is expressly consented to by the relevant person; or (b) the conditions of "deemed consent" are met and an adequate level of protection of personal data is ensured in the course of the processing of the transferred data in the third country. The conditions of "deemed consent" are as follows if obtaining the consent proves impossible or involves a disproportionate effort and the processing of personal data (a) is necessary for compliance with a legal obligation applicable to the data processor; or (b) the processing is necessary for the purpose of legitimate interests of the data processor or third parties, and such necessity is proportionate to the restriction of privacy. Certain countries have been deemed adequate by the

	European Commission (e.g. Switzerland, Argentina). The United States is not deemed to have adequate protection, but has in place the Safe Harbor Program, which is deemed sufficient if the relevant company has signed up to this. In other cases, the European Commission-approved model contractual clauses shall be used to ensure adequate protection. The employees shall also be informed that the other country may not ensure adequate protection. In addition, this data transfer outside the EEA shall be registered with the Hungarian Data Protection Supervisory Authority (until 1 January 2012, the Information Commissioner).

Duties of the employer connected with termination of an employment contract

Are there any duties relating to data protection connected with the termination of an employment contract?	There is no law stipulating obligation on this. At the employee's request, the employer shall – either at the time of termination (cessation) of the employment relationship, or in any case within one year after that time – provide a written assessment of the employee's work if the employment relationship has lasted for at least one year. If the assessment contains any false facts, the employee may bring an action before the court to have such facts abolished or revised. According to the Information Commissioner, as of the termination date, the business e-mail address and other direct contact channels of the employee should be terminated. The senders of any incoming e-mails and any other form of communication should be informed that: (i) the employee no longer works for the employer, and the employee shall be contacted in other ways of communication regarding private matters; and (ii) in case of business issues, the sender shall contact the relevant person at the employer.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	There is no law stipulating obligation on this. Although companies must ensure they do not retain the personal data of former employees once there is no longer a legitimate business need or legal requirement to do so, in practice it is advisable to keep HR documentation – e.g. documents certifying employment-related claims, the termination letter, and employment agreement, for three to five years from the due date of the claims. (Unless the documents are needed for taxation or accounting, in which case a mandatory longer retention period of ten years applies.)

Contacts

Contacts within own jurisdiction	Márton Domokos **E** marton.domokos@cms-cmck.com Dora Petrányi **E** dora.petranyi@cms-cmck.com
Contacts within jurisdictions different from that mentioned in this list	

Italy



Group contact: Fabrizio Spagnolo

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	Yes, if the employer allows this.
Are there any specific requirements for doing so?	If the employer intends to forbid or regulate the use of internet for private purposes, the Italian Garante suggests the adoption of certain specific measures. The most relevant of these is the use of filters to prevent certain operations considered to be unrelated to the work being performed by the employee.
Is the employee allowed to use his/her office e-mail account for private purposes?	No. It is forbidden for the employee to use the office e-mail account for private purposes.
Are there any specific requirements for doing so?	In order to avoid any incorrect use of the electronic tools of the company, the Italian Garante suggests that the employer provide a specific e-mail account which can be used by employees for private purposes.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	According to the Italian Privacy Garante, the employer's controls are only lawful if the principles of relevance and non-excessiveness are complied with. The employer can only impose controls on aggregate data related to the whole establishment or specific units thereof.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	Yes. In this case, the employer is not allowed to check employee's e-mails.
Data collection during the application process	
What information is the employer allowed to collect?	The employer cannot collect data if this contains information that could be used to discriminate against the employee, or if it is not necessary for the performance of his/her legal or contractual duties.
How long may data of this nature be stored?	According to the Italian Data Protection Code, personal data should be stored for no longer than is necessary for the purpose for which the data was collected and subsequently processed.

Is the consent of the employee required?	For data contained in public registers, lists, acts and documents which are already publicly available, the consent of the applicant is not necessary. Consent is always required if the treatment concerns sensitive data, however.
GPS tracking	
Under what conditions can the employer use GPS tracking?	According to Art. 4 of Italian Law nr. 300/1970, the use of equipment with the aim of realising remote control of the employee is forbidden.
Use of video surveillance	
Is the employer allowed to use video surveillance?	It is forbidden to use audio or video systems to control the activity of an employee at a distance, except if these equipments are considered necessary to satisfy organisational and productive reasons, or to guarantee safety conditions at work.
Are there any specific requirements for doing so?	It is specifically requested that the equipment can only be installed if previously agreed with the unions, or in case of non-agreement, if authorised by the competent labour authorities ("Ispettorato del Lavoro").
Are there any situations/ locations where video surveillance is generally prohibited?	No. The use of audiovisual instruments is always forbidden if their installation is not justified for organisational or productive reasons.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	If personal data are available on the internet or contained in a publicly available document, then they can be used and verified directly by the employer.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	No. The employer can only regulate the use of internet and social media in the workplace.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	The Italian Data Protection Code provides an efficient regulation in order to ensure the dignity and all fundamental rights of the employee are respected. The Code also allows the employer to control the appropriate use of worktools by employees for purposes related to the work being done.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	The prior agreement of the works council is not necessary to collect an employee's personal data. The employer shall be bound to respect the provisions defined for the processing of personal data, even if a prior agreement with the works council is in place.
To what extent can data collection, processing and use be justified by agreements with unions?	Prior agreement with the unions is not necessary to collect employee's personal data. The employer is bound to respect the provisions provided for the process of personal data, even if a prior agreement is in place with the unions.

Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	No. The employer is bound to respect provisions defining the processing personal data, even if the employee has already provided his consent.
If so, to what extent?	Not applicable.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	Not applicable.
What kind of participation rights do unions have in relation to data protection?	According to L.300/1970, the employer is required to come to an agreement with unions if he intends to use audiovisual equipment with the aim of gaining remote control over employees, or before proceeding to personal inspection of the employee.
Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	Transfer of personal data to third countries is regulated by Arts. 42 and 43 of the Italian Data Protection Code.
What are the requirements for data transfer to take place within a group?	According to Art. 43 of the Code, personal data subject to processing may be transferred from the State's territory to countries outside the European Union under specific conditions, the most relevant being that the employee must give his/her consent, either expressly or, where the transfer concerns sensitive data, in writing.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	Yes, the Italian Data Protection Code provides specific rules for data transfer, according to which there are different provisions if the country is a Member State of the EU or a third country.
Duties of the employer connected with termination of an employment contract	
Are there any duties relating to data protection connected with the termination of an employment contract?	If an employment contract is terminated, the employer should delete any data no longer necessary for the purposes for which the data was collected or subsequently processed.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	According to the Italian Data Protection Code, personal data processed for any purpose should not be kept longer than necessary for the given purpose.
Contacts	
Contacts within own jurisdiction	
Contacts within jurisdictions different from that mentioned in this list	

Luxembourg



Group contact: Julien Leclère

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	Yes, reasonable use of the internet for private purposes at work may be available to employees.
Are there any specific requirements for doing so?	If the employer wants to restrict or control use of the internet for private purposes, he must inform employees prior to putting any restrictions in place.
Is the employee allowed to use his/her office e-mail account for private purposes?	The employer cannot totally forbid the use of office e-mail for private purposes, and reasonable use by the employees is tolerated.
Are there any specific requirements for doing so?	The employee must mark all his personal e-mail(s) as "private" or "personal". Such e-mails cannot be opened by the employer without the employee being present. The employee has the right to deny such access to his/her personal files. If the employee's employment contract is terminated or he/she dies, the person responsible for the protected data should erase the former employee's personal files.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	The employee must mark all his personal e-mail(s) as "private" or "personal". Such e-mails cannot be opened by the employer without the employee being present. The employee has the right to deny such access to his/her personal files. If the employee's employment contract is terminated or he/she dies, the person responsible for the protected data should erase the former employee's personal files.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	Yes, employees' private e-mails cannot be inspected as stated above. There is one exception, however: when the inspection is authorised by a judge.
Data collection during the application process	
What information is the employer allowed to collect?	The employer is not allowed to collect information on racial or ethnic origin, political beliefs, religious or philosophical beliefs, union membership, as well as data on the health and sex life of the employee, including genetic data. In addition to these restrictions, the employer cannot collect judicial information.
How long may data of this nature be stored?	The storage of the data should not exceed the time necessary for the aim of the data collection to be achieved. In principle, this should be no longer than six months.
Is the consent of the employee required?	Yes

GPS tracking	
Under what conditions can the employer use GPS tracking?	The employer can use GPS tracking after requesting such authorisation to the "Commission Nationale de Protection des Données" ("CNPD") and only if it is necessary for: — Safety and health reasons; — Protecting goods of the company; — Controlling the manufacturing chain; — Temporary control of production or services performed by the employee, when the sole measure is to determine his/her remuneration; — Maintaining a flexible schedule for the employee.
Use of video surveillance	
Is the employer allowed to use video surveillance?	Yes, if he has requested such authorisation from the CNPD, the CNPD has allowed him to use it, and only if it is necessary for: — Safety and health reasons; — Protecting goods of the company; — Controlling the manufacturing chain; — Temporary control of production or services performed by the employee, when it is the sole measure to determine his/her remuneration; — Maintaining the flexible schedule of the employee.
Are there any specific requirements for doing so?	The employer must justify video surveillance for one of the reasons explained in GPS tracking, and must also: — Inform the employee of such surveillance; — Inform the mixed comittee, staff delegation or Ministry.
Are there any situations/ locations where video surveillance is generally prohibited?	Video surveillance is generally prohibited in areas where the employee has the right to privacy.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	Social media relating to a job applicant may not be used as a formal source.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	Social media relating to a job applicant may not be used as a formal source.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	There is no specific data protection law relating to efficiency controls, but various forms of controlling and monitoring efficiency will have data protection implications.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Not applicable.

To what extent can data collection, processing and use be justified by agreements with unions?	Not applicable.

Justification by consent of the employee

Can the regulations of data protection law be altered by consent of the employee?	No, the consent of an employee cannot legitimate a treatment which does not respect the provisions of data protection law.
If so, to what extent?	Not applicable.

Participation rights of the works council and unions

What kind of participation rights do works councils have relating to data protection?	The works council/mixed committee must give its approval prior to the CNPD in some cases of monitoring of employees.
What kind of participation rights do unions have in relation to data protection?	

Data transfer within a group

Does data protection law provide for any special regulations relating to data transfer within a group?	The law does not provide for any regulations relating to data transfer within a group, but within third party countries.
What are the requirements for data transfer to take place within a group?	This depends whether the data is transferred within the EU or not.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	Within the EU: no special requirement. Outside the EU: the CNPD must be informed if the third country does not provide adequate protection of the data, unless the law derogates to this rule (e.g. if the transfer is necessary for the execution of a contract to which the employee is party to, etc.).

Duties of the employer connected with termination of an employment contract

Are there any duties relating to data protection connected with the termination of an employment contract?	There are no special duties. Only those stated above in the case of an employee's termination of the employment contract, when the person responsible for the protected data must erase the former employee's personal files.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	Information relating to an employee cannot be kept for a longer period than that necessary to achieve the purpose for which the data has been collected.

Contacts

Contacts within own jurisdiction	Julien Leclere **E** julien.leclere@cms-dblux.com Jérôme Pascua **E** jerome.pascua@cms-dblux.com
Contacts within jurisdictions different from that mentioned in this list	

The Netherlands



Group contact: Katja van Kranenburg-Hanspians

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	The employer must accept private use of the internet by employees to a certain extent, as long as it is not interfering with the employee's work or the work of his colleagues, and is not harmful to the company. Excessive or inappropriate use is not allowed.
Are there any specific requirements for doing so?	No, although the employee will need to act within the boundaries of what may be expected of a good employee (7:611, Dutch Civil Code). However, the employer can lay down rules and regulations regarding the extent and nature of private internet use. It is important that these rules and regulations are communicated to the employee and consequently enforced by the employer. These parameters can also be built into company software by such measures as contentfiltering, the blocking of certain websites, and use of available software programs.
Is the employee allowed to use his/her office e-mail account for private purposes?	The employer must accept private use of the office e-mail account by employees to a certain extent, as long as it is not interfering with the employee's work or the work of his colleagues, and is not harmful to the company. Excessive or inappropriate use is not allowed. Stricter rules may apply to the use of the business e-mail account if the employer provides the employee with a separate e-mail account for private use.
Are there any specific requirements for doing so?	No, although the employee will need to act within the boundaries of what may be expected of a good employee (7:611, Dutch Civil Code). The employer can lay down rules and regulations regarding the extent and nature of private use of the office e-mail account. These parameters can also be built into company software by such measures as contentfiltering.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	The employer may monitor e-mail usage by employees for a previously determined goal (such as compliance with the ICT code of conduct) and limited to monitoring mechanisms designed to achieve that goal. Monitoring and logging of data shall be limited as much as possible. Both the logging of an analysis of traffic data and the monitoring of any content being exchanged by an employee are only permitted if necessary to protect an interest of the employer which outweighs the employee's privacy interest. In addition, the employee should be informed in advance. The processing of personal data should be minimised to what is strictly necessary to achieve the objective of the monitoring, and data must be adequately protected. As a rule, monitoring systems must be subjected to a privacy impact assessment, and "privacy by design" principles applied when developing and implementing the system. Data must not be stored for longer than necessary.

	Ad hoc checking of e-mail messages is allowed where there is suspicion of serious misbehaviour, such as fraud or corruption. In these cases, the employee must be notified as soon as the investigation allows. Privileged communications (with the works council or company doctor, for example) shall be excluded wherever possible. Decisions regarding the establishment, amendment or cancellation of a monitoring system are subject to the consent of the works council.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	The employer must avoid unnecessary monitoring of private e-mails. Private e-mail needs to be excluded from monitoring unless the employer has a specific reason for viewing such e-mails, such as well-founded suspicion of misbehaviour. If the employer has provided for a separation in business-related and private e-mail correspondence (e.g. two separate accounts), its monitoring powers in respect of the "business account" may be more far-reaching than in situations where the private and business e-mails are not processed separately.
Data collection during the application process	
What information is the employer allowed to collect?	Information relating directly to the (suitability of the applicant for the) job vacancy, such as basic details (name, address, date of birth), education and work experience. The collected data should not disproportionately infringe upon the privacy of the applicant.
How long may data of this nature be stored?	In general, the data may be stored for four weeks after the selection procedure has been terminated. Where the applicant has provided his/her prior written consent, data may be stored longer. A one-year period after termination of the selection proceedings is considered reasonable by the Dutch Data Protection Authority (DDPA) in this case.
Is the consent of the employee required?	No, unless an extended storage term is agreed upon. See above.
GPS tracking	
Under what conditions can the employer use GPS tracking?	This is allowed if necessary and proportionate for the protection of a legitimate interest of the employer (which must outweigh the privacy interests of the employee). The employee should be informed that GPS tracking takes place. Such processing is only permitted if the GPS tracking is necessary and proportionate to a specific goal (e.g. the protection of employees against hijacking). The establishment, amendment and cancellation of rules and regulations regarding GPS tracking are subject to the consent of the works council. The DDPA must also be informed of relevant data processing activities prior to commencement.
Use of video surveillance	
Is the employer allowed to use video surveillance?	Yes, if the requirements mentioned below are met.
Are there any specific requirements for doing so?	Visible video surveillance: allowed if necessary for the protection of a legitimate interest of the employer (which must outweigh the privacy interests of the employee). Hidden video surveillance: not allowed in principle. Under some circumstances (e.g. theft of company property), the employer may have a legitimate interest in using hidden video surveillance under very strict conditions. Employees must be notified in advance that the employer may use (hidden) video surveillance and also as soon as possible after the hidden video surveillance takes place. The works council has a right of consent with regard to company regulations on (hidden) video surveillance. The employer must also notify the DDPA.

	When video surveillance is (only) used for the protection of people, buildings or goods, there is no obligation to notify the DDPA. Evidence obtained in breach of data protection law is often nonetheless accepted in civil proceedings, but this does not repair or justify the breach of data protection law, or the employer's exposure to (criminal) sanctions.
Are there any situations/ locations where video surveillance is generally prohibited?	Video surveillance in non-public areas, such as dressing rooms, is generally prohibited.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	The employer should exercise restraint in using social media as a source for information. In principle, information should be requested from the applicant or prior approval should be obtained from the applicant for social media to be used.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	The employer can lay down rules and regulations in its code of conduct. The extent to which these directions can be enforced will be dependent, amongst other things, on the position of the employee within the company.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	The general rule that the collection of personal data should be necessary and proportionate applies. The works council has a right of consent regarding rules and regulations governing use of personnel monitoring systems controlling attendance, behaviour and performance.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	The argument that data collection, processing and use are based on agreements with works councils (which will have a right to consent in most cases) may contribute to the conclusion that data collection, processing and use is necessary and proportional.
To what extent can data collection, processing and use be justified by agreements with unions?	The argument that data collection, processing and use are based on agreements with unions (which will have a right to consent in most cases) may contribute to the conclusion that data collection, processing and use is necessary and proportional.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	Dutch data privacy law stipulates that data processing is justified if the data subject has granted its consent. Given the dependent position of the employee, however, the general assumption is that the employee cannot effectively grant such consent as this is not considered to have been 'freely' given. There are certain exceptions to this rule, in situations where the employer can demonstrate that withholding or withdrawing consent has no consequences whatsoever.
If so, to what extent?	See above.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	The works council has a right of consent regarding decisions on the establishment, amendment or cancellation of rules and regulations governing the processing and protection of personal data of employees of the enterprise, complaints procedures and the monitoring of attendance, behaviour and performance by personnel.

	A decision taken by the entrepreneur without the prior consent of the works council is void if the works council invokes the nullity of that decision in writing within one month from the time the decision is brought to its attention. If the works council does not grant its consent, the entrepreneur can, after mediation of the Joint Sectoral Committee, ask the subdistrict court judge for permission to take said decision, in case the refusal by the works council to grant its consent is unreasonable, or the intended decision is necessitated for serious organisational, economic or social business reasons.
What kind of participation rights do unions have in relation to data protection?	Unions have no statutory participation rights. The employer shall check the provisions of the applicable CLA, if any, to see if any specific conditions have been agreed therein.

Data transfer within a group

Does data protection law provide for any special regulations relating to data transfer within a group?	The DDPA does not provide any specific rules for inter-company transfer of personal data. As a result, any transfer to another group company must be assessed against the statutory requirements of the DDPA. However, the need to share certain information with other entities within the group of companies of the data controller may qualify as a statutory justification ground.
What are the requirements for data transfer to take place within a group?	See above. Transferring personal data to recipients within the group of companies to which the data processor belongs is only permitted if such transfer is necessary for and proportionate to the purpose for which the data were processed.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	If personal data are transferred to group companies in countries without a suitable level of data protection, the employer must have the following in place: (i) data processor agreements using the European Commission approved model contractual clauses; or (ii) a data export permit from the Ministry of Justice, for example if the employer uses Binding Corporate Rules which are approved by one of the data protection authorities that takes part in the mutual recognition program.

Duties of the employer connected with termination of an employment contract

Are there any duties relating to data protection connected with the termination of an employment contract?	No, the Dutch Data Protection Act remains in full force.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	In general, the information is disposed of two years after the termination of the employment contract, unless another statutory retention period applies (e.g. for tax purposes).

Contacts

Contacts within own jurisdiction	Wouter Seinen **E** wouter.seinen@cms-dsb.com Stephanie Dekker **E** stephanie.dekker@cms-dsb.com
Contacts within jurisdictions different from that mentioned in this list	

Poland



Group contact: Katarzyna Dulewicz

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	There are no legal provisions prohibiting the use of the internet for private purposes under Polish law. However, excessive use of the internet for private purposes during working hours, or its use for commercial or offensive purposes, could be considered a breach of an employee's employment contract and entitle an employer to terminate such contract. It is common for employers to have a policy in place that either prohibits or regulates use of the internet.
Are there any specific requirements for doing so?	There are no specific requirements concerning use of the internet by employees for private purposes. If the employer wishes to set up such rules, howver, it should include them in work byelaws.
Is the employee allowed to use his/her office e-mail account for private purposes?	There are no legal provisions on using office e-mail accounts for private purposes. Employers often control such use through their own policies and rules (by including restrictions in work byelaws, for example).
Are there any specific requirements for doing so?	There are no specific requirements over whether employees should be allowed to use office e-mail accounts. If the employer wishes to set up such rules, howver, it should include them in work byelaws.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	Yes, the employer is allowed to check the employee's e-mails, but not private ones. Before doing so, the employer should notify employees that such checking will take place (such information may be included in the work byelaws). There are no specific provisions of law in this regard, but rules have been worked out in practice.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	In such cases, it is advisable to enable employees to mark each e-mail as "private" or "shared". An employer must not read employees' private e-mails. If an employer accesses private e-mails by accident, the e-mail content may not be shared with other employees or third parties, and the employer must not continue reading it.
Data collection during the application process	
What information is the employer allowed to collect?	The employer may collect the following information from candidate employees: first name (names), surname; parents' names; date of birth; residential address (address for correspondence); education and employment history.
How long may data of this nature be stored?	Personal data may be processed for no longer than necessary to achieve a legitimate purpose. In the case of candidate employees, an employer should only process personal data until the recruitment process is complete.

Is the consent of the employee required?	To process information within the scope of the law and for the purposes provided, a prospective employer is not required to gain an employee candidate's consent. An employee candidate's consent is necessary where he/she provides more information than required by law, or where the candidate would like to take part in further recruitment processes. The Polish data protection authority questions the legitimacy of an employee's consent in an employment relationship (due to its lack of a voluntary character).
GPS tracking	
Under what conditions can the employer use GPS tracking?	There are no specific provisions of law in this regard. In general, the employer may use GPS tracking. He has to inform an employee about the use of such system and the purpose of the tracking. At the request of the employee, the employer should provide him/her with the information collected by GPS tracking. Data collected using GPS tracking systems is considered personal data under Polish law.
Use of video surveillance	
Is the employer allowed to use video surveillance?	Yes.
Are there any specific requirements for doing so?	There are no specific provisions of law in this regard. An employee needs to be informed of the use of video surveillance. The surveillance can only be used to achieve legitimate purposes, and cannot be used in places such as toilets, cloakrooms or restrooms. According to the Polish data protection authority, data collected by means of video surveillance should be considered personal data.
Are there any situations/ locations where video surveillance is generally prohibited?	As video surveillance is not prohibited by law, general rules of data protection regulations and civil law apply. In practice, video surveillance should not take place in areas that employees would expect to be private, such as bathrooms, cloakrooms or restrooms.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	Provisions of Polish labour law do not allow a prospective employer to process more information about employee candidate than his/her first name, surname, date of birth, address, education and professional experience. By using social media (i.e. Facebook, Twitter), the employer gains access to a much wider scope of personal data, which is incompliant with Polish law.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	The employer may prohibit or limit use of the internet with respect to specific categories of websites, e.g. social media websites. However, the employer cannot influence the use of social media (in terms of content and scope) for private purposes after hours. In practice, there have been cases in which employees have been sacked for infringing upon the employer's rights by using social media.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	No. As the employer cannot breach the employee's right to privacy and dignity, any means undertaken to control efficiency must be necessary and proportional to such purpose. Some forms of monitoring efficiency may have data protection implications.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Agreements with works councils should not change the rules governing personal data processing.

To what extent can data collection, processing and use be justified by agreements with unions?	Agreements with unions should not change the rules governing personal data processing. If employees are members of trade unions, the employer will be entitled to process more information about those employees (subject to fulfilling additional requirements).
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	Consent cannot alter the regulations of law. For more information, please see the answers above. In practice (although this carries some risk), employers ask employees to consent to transferring their personal data to other companies of the employer's group or third countries.
If so, to what extent?	Not applicable.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	None.
What kind of participation rights do unions have in relation to data protection?	None.
Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	No, data transfer within a group is not regulated any differently than regular data transfer between an employer and a third party. In the event of such a transfer, all legal requirements need to be fulfilled, without exception.
What are the requirements for data transfer to take place within a group?	This is possible, subject tothe same conditions as data transfer between an employer and a third party (not belonging to the group).
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	Transferring personal data between a company located in Poland to a company located outside the European Economic Area is subject to additional requirements (e.g. legal basis and consent from Polish data protection authority).
Duties of the employer connected with termination of an employment contract	
Are there any duties relating to data protection connected with the termination of an employment contract?	Under Polish law, an employer is required to archive information about employment contracts, salaries, attendance and other categories of information relating to former employees.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	An employer is obliged to keep documents essential to provide former employees with social insurance. The employer has to keep such information for 50 years. Schedules, time-tracks and attendance lists should be kept for between two and 25 years.
Contacts	
Contacts within own jurisdiction	Katarzyna Dulewicz **E** katarzyna.dulewicz@cms-cmck.com
Contacts within jurisdictions different from that mentioned in this list	

Portugal



Group contact: Susana Afonso Costa

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	There is no law regulating use of the internet at work for private purposes. The employer has the right to decide whether employees can use the internet for private purposes or not, and restrict access to the internet. Normally this use is regulated by internal policies and rules or works agreements. If use is not regulated by the employer, private use is admissible as long as it is kept within an ordinary and marginal limit. In cases where the use of internet for private purposes is forbidden or is excessive during working hours, or even if used for commercial or offensive purposes, it could be considered a breach of an employee's employment contract being subject to a disciplinary procedure.
Are there any specific requirements for doing so?	There are no specific statutory requirements concerning such use. However, the employer must assure that the employee takes knowledge of the internal policies and rules or works agreements.
Is the employee allowed to use his/her office e-mail account for private purposes?	Unless instructed otherwise by the employer, he/she is allowed to do so. These instructions can be contained in the contract or, more frequently, in internal policies.
Are there any specific requirements for doing so?	If e-mail personal use is not forbidden, the employee must indicate which messages are private/personal, otherwise, the employer may assume and will assume that the message is not personal/private.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	According to the Portuguese Labour Code the employee is entitled to reserve and the confidentiality of contents of personal messages and access to non-professional information sent, received or consulted, namely through e-mail. Notwithstanding, such rule does not affect the employer's right to establish rules regarding the use of the undertaking's electronic resources, namely e-mail. Therefore, even in cases where the e-mail use for personal purposes is forbidden, and assumed that all e-mails are of professional content, it is not allowed the employer to check its content if the e-mails subject suggests to be of private content. In fact, it is understood that whenever an employer realizes that the content is personal, he must immediately stop its reading. We do alert to the fact that according to the Portuguese Criminal Code the disrespect of such conduct is understood as crime of violation of correspondence.

	Please note that the employer may always resort to the punishable measures previewed in the Portuguese Labour Code in case of misconduct by the employee. We also alert to the fact that the e-mail content may not be used as prove, as it will be considered void according to the Portuguese Constitutional Law. Last but not least, the employer must assure that the employee takes knowledge of the internal policies and rules or works agreements where it is established the possibility of the employer to check the e-mails content.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	Please refer to the previous answer.
Data collection during the application process	
What information is the employer allowed to collect?	According to the Portuguese Labour Code the employer cannot require job candidates or employees to provide information regarding the employee's private life, state of health or pregnancy except when such information is strictly necessary and relevant to assess their capability to perform the employment contract and such grounds are supplied in writing. Any information regarding state of health or pregnancy may only be provided to doctors that will confirm or not confirm the employee's aptitude to work. Having this in mind, the data collected must be adequate, relevant, not excessive and accurate.
How long may data of this nature be stored?	All entities must keep during five years all processes of recruitment.
Is the consent of the employee required?	The express consent of the employee is always required, except in situations of execution of the employment contract. Despite this, the employer must inform the employee of what data are to be collected, and make clear the employee's rights of access, rectification, opposition and cancellation.
GPS tracking	
Under what conditions can the employer use GPS tracking?	Only if such tracking is proportional and necessary for the development of the professional activity. It is always necessary the Data Protection Agency's authorization to produce effects. If and the Data Protection Agency authorizes, the employee that is going to be tracked must always be notified. Please note the GPS tracking may not be used to control the employee's performance of work.
Use of video surveillance	
Is the employer allowed to use video surveillance?	Yes, but only to protection toward third parties, and once issued the necessary authorization by the Data Protection Agency. It may not be used to control the employee's performance of work.
Are there any specific requirements for doing so?	Yes. In order to proceed with the video surveillance, the employer must request and have a permission issued by the Data Protection Agency. Upon the request of the referred authorization, the employer must also send the works council's written opinion. Also, the employer must inform the employee of the cameras installation and its purposes, as well as inform in written and locally the following information: *"This place is under surveillance of a closed circuit television"* or *"This place is under surveillance of a closed circuit television, proceeding to image and sound record".*

Are there any situations/ locations where video surveillance is generally prohibited?	It is generally prohibited in private areas such as toilets or private offices.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	If personal data are available on the internet or contained in a publicly available document, then they can be used and verified directly by the employer. However, it must always be assured a non-discrimination behavior by the employer.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	No. The employer can only regulate the use of internet and social media in the workplace.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	No. It will depend on the company's internal policies, and must always be proportional.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Agreements with works councils should not change the rules on personal data processing. The employer is always bound by Data Protection Law.
To what extent can data collection, processing and use be justified by agreements with unions?	Please refer to the proceeding point.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	Yes. However, the employee must be fully informed, give his consent free and expressly.
If so, to what extent?	As agreed between employer and employee.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	In data protection issues, only the employee is entitled to exercise his/her rights concerning personal data. Works councils may only give their written opinion regarding the use of video surveillance and use biometrical system to control punctuality.
What kind of participation rights do unions have in relation to data protection?	Not applicable.

Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	Data transfer within a group is not regulated any differently than regular data transfer between an employer and a third party. In the event of such a transfer, all legal requirements need to be fulfilled, without exception.
What are the requirements for data transfer to take place within a group?	Transfer to a group company is a form of data processing, and the employer must comply with the relevant legal requirements.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	Yes. A transfer of data to a country outside the EU requires that the other country ensures the same protection. In such cases it is necessary to have authorization issued by the Data Protection Agency.
Duties of the employer connected with termination of an employment contract	
Are there any duties relating to data protection connected with the termination of an employment contract?	Data will only be kept if considered necessary for the purpose for which it was initially collected. In this case, the information must be blocked by the employer. In case of termination of the employment contract or of transfer of work place, the employer is obliged to eliminate all biometrical data of the respective employee.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	All entities must keep during five years all processes of recruitment. According to the Portuguese Labour Code the employer must keep during five years all information regarding work time schedules, overtime records. According to the Portuguese Corporate Income Tax Code employers must keep during ten years all accountancy records of the company.
Contacts	
Contacts within own jurisdiction	Susana Afonso Costa **E** susana.afonso@cms-rpa.com
Contacts within jurisdictions different from that mentioned in this list	

Romania



Group contact: Marius Petroiu

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	There is no specific regulation restricting or prohibiting employees from accessing the internet for private purposes while at work. However the employer may restrict or prohibit the internet access for private purposes of its employees by means of internal policies or rules.
Are there any specific requirements for doing so?	There is no law imposing specific requirements preventing/allowing employees internet access for private purposes within a work context. The employer may therefore prevent or allow employees from using the internet at work by means of internal policies or rules.
Is the employee allowed to use his/her office e-mail account for private purposes?	There is no piece of legislation preventing/allowing the employee from using the office e-mail account for private purposes. In practice, however, employers may restrict private use of office e-mail accounts by employees by means of internal policies or rules.
Are there any specific requirements for doing so?	From the legislative perspective, such requirements do not exist, so limited to employer's internal policies or rules.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	If, by "checking" an employee's e-mail, the employer intentionally opens that e-mail, and becomes aware of the content as a result, and if the employer was not an intended addressee of the e-mail (the law takes into consideration only the situation when the person who checks for the e-mail is not the addressee), the employer may be held liable for committing the criminal offence of breaching the secrecy of correspondence. Nevertheless, further criminal proceedings will only be undertaken if the employee files a criminal complaint with the prosecutor's office.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	As stated above, the law does not distinguish the purpose of the communication. It only takes into consideration that the person who reads the e-mail is not an intended addressee, therefore making him possibly liable for a criminal offence.

Data collection during the application process

What information is the employer allowed to collect?

Data, amended and supplemented ("Law 677/2001") sets out the conditions under which an employer may collect such personal data. Data "collection" is a form of processing data, thus the following principles should be respected:

(i) the data should be processed without deceit;
(ii) the data should be collected for specific, explicit and legitimate purposes;
(iii) the data should be adequate, pertinent, and non-excessive in relation to the purpose for which they are collected and processed;
(iv) the data should be accurate and updated;
(v) the data should be stored in such a manner so as to allow the identification of the data subject only for the time limit required to fulfill the scope of processing.

For any personal data where processing is necessary:

(i) the person's express and unequivocal agreement (except for specific situations when such agreement is not required);
(ii) the person's information related to the scope of the data processing, as well as any other further details (e.g., the data beneficiaries, the rights the person has, etc.).

How long may data of this nature be stored?

A strict timeframe is not laid down; instead, Law 677/2001 refers to the period deemed necessary for processing data.

Is the consent of the employee required?

As a rule, one of the conditions imposed by Law 677/2001 for lawful data processing is to obtain from the data subject the express and unequivocal agreement for the envisaged processing.

GPS tracking

Under what conditions can the employer use GPS tracking?

Under the definition provided within Law 677/2001, it may be considered that GPS tracking is a form of personal data processing, as it may lead to identification of an individual. Moreover, the National Supervision of Personal Data Processing Authority ("NSPDPA") has issued its Decision 11/2009, according to which processing personal data that allows geographic localisation of individuals is deemed to present special risks for the freedoms and rights of those individuals. The NSPDPA must therefore be notified 30 calendar days before such data starts to be processed. Furthermore, being a form of data processing, the express and unequivocal agreement of the employee must be obtained.

Use of video surveillance

Is the employer allowed to use video surveillance?

The employer may legally use video surveillance if certain requirements as stated below are respected.

Are there any specific requirements for doing so?

According to Law 677/2001, video surveillance may be deemed a processing of personal data activity. The NSPDPA should therefore be notified of any video surveillance. The notification should include, amongst other things, the following information:

(i) the name of the data processing operator;
(ii) the scope of the video surveillance;
(iii) a description of the envisaged individuals or category of individuals and of the data or category of data to be processed;
(iv) the modality of informing the envisaged individuals;
(v) the beneficiaries or categories of beneficiaries to whom the collected data is to be disclosed;
(vi) data transfer, if applicable. It is also advisable to post a disclaimer regarding the use of video surveillance. Please note that the NSPDPA has drafted a decision regulating the protection of personal data processed through video surveillance, but this decision has not entered into force.

Are there any situations/ locations where video surveillance is generally prohibited?	The law is silent as regards this aspect. However, the Romanian Constitution (e.g. Article 26) and Article 8 of the ECHR protect the right to private life, and these articles may be interpreted as prohibiting the use of video surveillance in places that would be reasonably considered to be private (e.g., restrooms, locker areas, etc.).
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	There is no legal provision preventing this. Using social media to collect information about a job applicant is allowable, therefore, as long as the employer does not discriminate against the applicant based on the information collected via social media.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	Legislation does not prevent an employer from limiting or prohibiting use of social media at work. The recommended way of doing this is by means of internal rules or policies, which should be expressly accepted by employees.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	Efficiency controls are not covered by Law 677/2001. Nevertheless, the methods by means of which efficiency controls are carried out may require compliance with data protection law.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	The answer below referring to trade unions can also be applied to works councils.
To what extent can data collection, processing and use be justified by agreements with unions?	Under Romanian law, the express and unequivocal agreement of the employee must be obtained if personal data processing is to be used. From this standpoint, while an agreement with a trade union may be useful, it is insufficient to cover legal requirements.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	As shown above, the law requires the express and unequivocal consent of the data subject, including when "personal sensitive data" referring to race, ethnicity, political, religious or philosophical beliefs; sexual orientation, trade union membership or personal genetic data are subject to processing.
If so, to what extent?	Law 677/2001 defines exceptional situations when consent is not required to process personal data (excluding sensitive data). Furthermore, when processing personal sensitive data (as defined above) there are also a limited number of circumstances when consent is not required.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	The participation rights of works councils relating to data protection are not set automatically.
What kind of participation rights do unions have in relation to data protection?	The participation rights of trade unions relating to data protection are not set automatically

Data transfer within a group

Does data protection law provide for any special regulations relating to data transfer within a group?	There is no specific provision regulating the transfer of personal data within a group.
What are the requirements for data transfer to take place within a group?	In case of a transfer of data within a group located in Romania, the procedure to follow implies a notification filed with the NSPDPA. As data transfer is a procedure envisaged by the law as a form of processing, all processing requirements must be complied with.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	It is also necessary to file an authorisation request with the NSPDPA, and obtain the consent of the person whose data is being transferred, unless this is not required.

Duties of the employer connected with termination of an employment contract

Are there any duties relating to data protection connected with the termination of an employment contract?	How long the personal data should continue to be held by the employer should be assessed when the employment contract is terminated.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	As stated above, Law 677/2001 does not lay down a required timeframe for keeping the information. The law refers to the period deemed necessary for processing employee personal data. When the personal data is no longer necessary, unless the data subject has consented to forwarding the data to another destination or consented to further processing, the data will be: (i) destroyed; (ii) transferred to another data operator, provided that processing will have similar purposes to those of the former personal data processing; or (iii) transformed into anonymous data and stored exclusively for statistical, historical or scientific research.

Contacts

Contacts within own jurisdiction	Marius Petroiu **E** marius.petroiu@cms-cmck.com
Contacts within jurisdictions different from that mentioned in this list	



Russia

Group contact: Sergey Yuryev

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	There is no applicable legislation. Issues related to use of the internet shall be governed by labour contracts and internal policies approved by the employer, and communicated to employees in writing.
Are there any specific requirements for doing so?	No.
Is the employee allowed to use his/her office e-mail account for private purposes?	This depends on the terms and conditions of his/her labour contract, and the employer's internal policy related to use of the internet.
Are there any specific requirements for doing so?	No.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	The employer is authorised to do this if the following conditions are met: (i) there are relevant provisions in labour contracts, and the internal policy regulating the use of office e-mail accounts is communicated to the employees in due course; and (ii) the employee has granted direct written consent to this.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	If the employee is allowed to use an e-mail account for private purposes, the employer's right to check his/her e-mails may be challenged (since there may be a conflict with the employee's privacy rights).

Data collection during the application process	
What information is the employer allowed to collect?	Russian legislation provides that all information in respect of the employee shall be received from that employee. If the required information is not received from the employee, then the employer must notify the employee that it is going to obtain such information from the other source and obtain written consent from the employee to its doing so. There is also a limited list of documents established by the legislation which the employer may request from the employee. There is also a ban on collecting information relating to an individual's state of health, political, religious and other beliefs, private life, membership of social organisations and labour unions (subject to certain exceptions), as well as information about their 'private life' and 'family secrets' (the law does not define exactly what is understood by 'family secrets' or 'private life').

How long may data of this nature be stored?	As a general rule, the storage of personal data is allowed until the purposes of the personal data processing have been achieved (i.e. termination of labour relationships), unless otherwise provided by law (the law usually specifies a period for storage of some official documentation related to employment). It is also possible to extend the term of the storage based on an agreement with the data subjects (written consent is required), but this needs to be determined on a case-by-case basis.
Is the consent of the employee required?	No, as long as personal data have been obtained directly from the employee, have only been processed for the purpose of performing the labour contract by the employer, without transferring personal data to third parties (unless such a transfer is allowed by law), and no sensitive personal data is involved.
GPS tracking	
Under what conditions can the employer use GPS tracking?	This may be done: (i) if there are relevant provisions contained in employment contracts and internal policy; and (ii) the employee has granted his/her direct written consent.
Use of video surveillance	
Is the employer allowed to use video surveillance?	There is a lack of legal regulation in this field. Video surveillance is allowed subject to the following conditions: (i) employees have given their express consent to such surveillance; (ii) an internal policy on the matter is approved by the employer and communicated to employees in due course; (iii) video surveillance is used in workplace areas only (not in recreation areas, halls, toilets or similar); and (iv) video surveillance does not affect any rights of third parties (clients). We also believe employers need to use video surveillance on a reasonable basis, and protect any data obtained (not make it publicly available, etc.).
Are there any specific requirements for doing so?	No express requirements are provided by law. As this qualifies as personal data collection, however, the measures indicated above need to be taken.
Are there any situations/ locations where video surveillance is generally prohibited?	Please see Points (iii) and (iv) in the answer to 'Is the employer allowed to use video surveillance'.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	There is a lack of legal regulation in this field. We believe that social media may be used as a source of information about a job applicant, provided that: (i) the social media source is in the public domain (no registration or similar procedures are needed to access such information); (ii) the employer does not take any decisions affecting the applicant on the basis of such information; and (iii) the employer only aims to obtain information relevant to labour relationships.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	We believe this is possible (by means of contracts of employment and internal policies), but such limitations may only apply during work.

Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	No.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Not applicable in Russia, as no direct regulation in this respect.
To what extent can data collection, processing and use be justified by agreements with unions?	Not applicable in Russia, as no direct regulation in this respect.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	No, not possible.
If so, to what extent?	Not applicable.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	Unions may require information from an employer with respect to its compliance with applicable data protection legislation, and subsequently enforce such compliance by legal means.
What kind of participation rights do unions have in relation to data protection?	The Labour Code provides that the employer, employees and their representatives (i.e. unions) shall jointly develop the measures aimed at protecting personal data.
Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	No.
What are the requirements for data transfer to take place within a group?	Data subject's consent in writing. The purpose of the transfer must also meet the requirements of the Labour Code (such a transfer is lawful if it is aimed at complying with Russian law, assists with employment, education and promotion, ensures the safety of employees, and exercises control over the quality of work performed), as well as the requirements of the Law On Personal Data.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	The transfer of personal data to a country that does not provide for an adequate level of protection of personal data requires written consent from the data subjects. So far there is no further guidance on this issue.

Duties of the employer connected with termination of an employment contract

Are there any duties relating to data protection connected with the termination of an employment contract?	As a general rule, the processing of personal data is allowed until the purposes of such processing (i.e. termination of labour relationships) have been achieved, unless otherwise provided by law (the law may define a period of time for storage of official documentation related to employment), or by the labour agreement. It is possible to extend the term of such processing on the basis of an agreement with the data subjects, but this needs to be addressed on a case-by-case basis. If personal data are lawfully kept by the employer after a labour contract has been terminated, the employer must take the same measures to protect such data as taken for the personal data of current employees.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	See above.

Contacts

Contacts within own jurisdiction	Sergey Yuryev **E** sergey.yuryev@cmslegal.ru
Contacts within jurisdictions different from that mentioned in this list	

Serbia



Group contact: Ksenija Ivetic, Radivoje Petrikić

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	This matter is not explicitly regulated by the law. Therefore, we believe that the answer is "yes" unless it is banned/limited by the employer. Please note that practice regarding personal data protection in Serbia is undeveloped since the law has only been actively applied for around three years.
Are there any specific requirements for doing so?	Since this matter is not regulated, there are no specific requirements for doing so.
Is the employee allowed to use his/her office e-mail account for private purposes?	This matter is not explicitly regulated by the law. According to unofficial information from the Commissioner for Information of Public Importance and Personal Data Protection (hereinafter the "Commissioner"), it is allowed, as it would be unreasonable to forbid the use of an office e-mail account for private purposes.
Are there any specific requirements for doing so?	Since it is not regulated, there are no specific requirements to do so.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	This matter is not explicitly regulated by the law. Since it is not regulated there are no specific requirements for doing so. According to unofficial information from the Commissioner, checking an employee's e-mail is forbidden in general, other than when the e-mail breaches another, prevailing constitutional right, or subject to specified conditions agreed with the employer.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	Not applicable.
Data collection during the application process	
What information is the employer allowed to collect?	The law does not explicitly define what information may be collected during the application process. The collection must be reasonable, however, in light of the purpose of the collection and further processing of personal data.
How long may data of this nature be stored?	In general, personal data protection law stipulates that storage and processing is allowed until the purpose of collection is fulfilled. It may therefore be presumed that the storage is allowed until the employment process is complete.
Is the consent of the employee required?	According to unofficial information from the Commissioner, the consent of the applicant is not required, but if data relating to persons who are not employed are stored/processed after the employment process is complete, then consent would be required.

GPS tracking	
Under what conditions can the employer use GPS tracking?	This matter is not explicitly regulated by the law. According to unofficial information from the Commissioner, the employee would have to be informed that GPS was being used, and if the vehicle is used for private purposes too, then the employee should be enabled to switch off the GPS device.
Use of video surveillance	
Is the employer allowed to use video surveillance?	This matter is not explicitly regulated by the law, but video surveillance is used in practice (at banks, stores, etc.).
Are there any specific requirements for doing so?	Since this matter is not regulated, there are no specific requirements to do so, but according to unofficial information from the Commissioner, employees must be notified of the existence of video surveillance systems.
Are there any situations/ locations where video surveillance is generally prohibited?	Since this matter is not regulated, there are no specific requirements to that regard.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	This matter is not explicitly regulated by the law, but personal data published on social media (e.g. Facebook, LinkedIn, etc.) by persons with full legal capacity are not subject to protection by the law, so the employer could use such information.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	This matter is not explicitly regulated by the law, but our understanding is that regulation of use of social media may be considered to be part of an employer's requirements regarding workplace discipline.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	No
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	The Personal Data Protection Law does not provide for this possibility.
To what extent can data collection, processing and use be justified by agreements with unions?	The Personal Data Protection Law does not provide for this possibility.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	No. The consent of the employee can only allow processing of personal data for purposes not provided for by law. Even this processing must be proportionate.
If so, to what extent?	Not applicable.

Participation rights of the works council and unions

What kind of participation rights do works councils have relating to data protection?	Works councils do not operate in Serbia.
What kind of participation rights do unions have in relation to data protection?	The Personal Data Protection Law does not regulate this matter, and our understanding is that unions do not have any significant rights regarding the processing of personal data of employees. The unions could only point out possible breaches regarding personal data protection (if noticed or reported by the employees), and ask the employer to correct these.

Data transfer within a group

Does data protection law provide for any special regulations relating to data transfer within a group?	No. All group companies are treated as separate companies.
What are the requirements for data transfer to take place within a group?	Data transfer within a group is subject to general requirements regarding the transfer of personal data.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	It does not make a difference if it is a group company or not, but in general, it does make a difference if the data are transferred to an EU Member State or not. If personal data are transferred from Serbia to a state party to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter the "Convention"), then approval of the transfer from the Commissioner is not required, while such approval is required if personal data are transferred to a country which is not a party to the Convention.

Duties of the employer connected with termination of an employment contract

Are there any duties relating to data protection connected with the termination of an employment contract?	In general, no.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	Personal data concerning employees which are collected and processed subject to the Law on Records related to Employment are kept permanently, while other personal data, collected and processed with the consent of the employee, are kept in accordance with the purpose for which are collected (the period of time for which data may be stored/processed depends on the purpose for which the data have been collected).

Contacts

Contacts within own jurisdiction	Radivoje Petrikić **E** radivoje.petrikic@cms-rrh.com Vesna Baric **E** vesna.baric@cms-rrh.com
Contacts within jurisdictions different from that mentioned in this list	Montenegro: Radivoje Petrikić **E** radivoje.petrikic@cms-rrh.com Milica Popovic **E** milica.popovic@cms-rrh.com

Slovakia



Group contact: Sylvia Szabó, Hana Supeková

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	This is not exactly prohibited, but the employee has to spend his working time performing the work of the employer, and not using the internet for private purposes. Such behaviour may be considered a breach of working discipline by the employer that could even result in dismissal.
Are there any specific requirements for doing so?	Use of internet for private purposes must be allowed by employers.
Is the employee allowed to use his/her office e-mail account for private purposes?	This depends on the employer, and if it allows its employees to use office e-mail for private purposes. In general, the computers and any tools provided for the employee to perform his/her work should be used for working. Such behaviour may be considered a breach of working discipline by the employer that could even result in dismissal.
Are there any specific requirements for doing so?	Using office e-mail for private purposes must be allowed by employers.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	If an employer intends to control e-mails of employees, it must inform them in advance of the extent of the control methods, how they are to be implemented, and their duration. Such control mechanisms must be discussed with the employees´ representative before being implemented. An employer may not intrude upon its employees' privacy at the workplace without serious reason. Generally, any natural person enjoys the rights protected under Slovak laws, such as the right to privacy, as anchored in the legal system of the Slovak Republic (Constitution of the Slovak Republic, Civil Code, etc.) and protected by international covenants on the protection of fundamental rights and freedoms (Charter of Fundamental Rights of the European Union, Convention for the Protection of Human Rights and Fundamental Freedoms, etc.). These rights protect the immunity of individuals, as well as their privacy, which includes postal secrecy, secrecy of transported messages and other written documents, and personal data protection. Considering that computers contain e-mails and data files carrying information of a private nature of any third person as well (other than an employee), control would constitute a breach of privacy law, data protection law and the right to post secrecy, and the secrecy of transported messages. An employer may only control e-mails where a serious reason for doing so exists, and must inform employees in advance of the controlling mechanism. When doing so, we also advise employers to ask their employees for confirmation that no personal data of third persons are in their e-mails. If this is the case, employers will need those third persons to consent to the storage and processing of their personal data.

If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	No, the previous also applies in this case. If an e-mail is marked as "private", the employer may not check it.
Data collection during the application process	
What information is the employer allowed to collect?	An employer may only collect and process personal data relating to the qualifications and professional experience of the employee, and data that may be relevant to the work carried out by the employee. The employer may also collect personal data necessary for it to perform its duties as an employer, e.g. bank details, wage levels, etc.
How long may data of this nature be stored?	Personal data may only be collected where the purpose of processing of personal data still exists. In the case of the personal data of employees, the purpose may also exist when the employment relationship has already been terminated. Based on several acts, regarding social insurance, health insurance and income tax, for example, documents containing personal data must be stored by the employer for up to ten years after the termination of the employment relationship.
Is the consent of the employee required?	The consent of employees to the processing of personal data is only necessary if the personal data being processed by the employer do not relate to the professional skills of the employee, or are not necessary for the employer to perform its duties according to the employment agreement concluded with the employee. The data necessary for the performance of the employment agreement are as follows: name, surname, title, date of birth, salary, bank account nr., etc. Consent is also required if the personal data are to be used by the employer for a purpose arising from the duty of the employer to perform his duties under the employment agreement. When the personal data of employees are used for marketing purposes, the consent of the employees involved is required.
GPS tracking	
Under what conditions can the employer use GPS tracking?	GPS tracking is considered a control mechanism. The employer must inform employees of the extent of the control methods, their implementation and duration, and must discuss the control mechanism with employees' representatives. An employer may not intrude upon employee privacy in the workplace without serious reason GPS tracking may only be used during the working hours of the employee, and if the serious reason exists. We recommend that GPS tracking be avoided, and another method of controlling employees used, such as controlling them at a particular position according to their route plans.
Use of video surveillance	
Is the employer allowed to use video surveillance?	The same principle applies here as in the case of e-mail checking described above. Employees must be informed of the planned mechanism of the control, but such control may not intrude upon the employee's privacy at the workplace without serious reason.
Are there any specific requirements for doing so?	Yes; employees must be notified that video surveillance is being used, and there must be a serious reason for putting such a system in place.
Are there any situations/ locations where video surveillance is generally prohibited?	This is not precisely defined in law, but in general it should be prohibited in situations/locations where the intimate sphere of the employee is infringed.

Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	Yes, using social media is not prohibited.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	It is allowed to prohibit access to social media from computers at work. Such use of social media during working hours may be considered a breach of workplace discipline. After work, the employer may not regulate the free time of its employees or how they spend it. It is possible to prohibit the content, to the extent that employees may not share information relating to their work because of the confidentiality of such information. Under the law, employees are obliged to maintain confidentiality regarding matters they have become acquainted with in the course of their employment, and which may not be disclosed to others in the interests of the employer. Also, persons and employees may not act in contradiction of the justified interests of the employer.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	No. The only reference to this is in the Labour Code, which states that an employer may control its employees where serious reason exists, but that the employer must notify its employees in advance of the control mechanism.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Advance discussion with employee representative bodies is required. If works councils and unions are working together at the place of work, the works council has the right to discuss the control mechanism before it is implemented.
To what extent can data collection, processing and use be justified by agreements with unions?	Advance discussion with employee representative bodies is required. If works councils and unions are working together at the place of work, the works council has the right to discuss the control mechanism before it is implemented.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	No, but it is possible to process even sensitive data with the written consent of employees, as this is allowed under the law. If personal data are to be transferred to a processor in a third country which does not provide an adequate level of protection, the consent of the DPA is required, even if employees have consented to soothe data being sent.
If so, to what extent?	Not applicable.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	Employee representatives' bodies, e.g. works councils, control the maintenance of labour regulations, including those relating to data processing, and request that the employer remove any faults discovered.
What kind of participation rights do unions have in relation to data protection?	Employee representatives' bodies, e.g. unions, control the maintenance of labour regulations, including those relating to data processing, and request that the employer remove any faults discovered.

Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	No. Even when personal data are transferred to another entity within the group, such an entity is treated as a third party.
What are the requirements for data transfer to take place within a group?	No special regulations or less strict regulation applies. In general, the consent of the data subject to the transfer of personal data is required, and the consent of the DPA is necessary when transferring personal data to a processor in a third country which does not ensure an adequate level of protection for the personal data.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	Yes, but it is not the fact that the entity is from a single group that makes a difference. The difference is in the final destination, and whether this is an EU country or a third country. In general, the written consent of the data subject is required for their personal data to be transferred to a third country which does not ensure an adequate level of protection, and the consent of the DPA is necessary when personal data are transferring to an entity carrying out the processing in such a country.
Duties of the employer connected with termination of an employment contract	
Are there any duties relating to data protection connected with the termination of an employment contract?	Once the purpose of processing the personal data has been achieved, the controller must destroy the personal data, unless a special law exists under which the employer is obliged to keep them. The controller should notify the data subject within 30 days of the fact that his/her personal data have been destroyed. Notification may be abandoned as long as the rights of the data subject are not violated by such abandonment of notification of destruction.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	Storage of the information depends on several special laws, and may extend up to ten years.
Contacts	
Contacts within own jurisdiction	Sylvia Szabó **E** sylvia.szabo@rc-cms.sk Hana Supeková **E** hana.supekova@rc-cms.sk
Contacts within jurisdictions different from that mentioned in this list	

Slovenia



Group contact: Dunja Jandl

Use of e-mail and the internet

Are employees allowed to use the internet for private purposes?

There are no provisions under Slovenian law prohibiting use of the internet for private purposes at the workplace. According to the Slovenian Personal Data Protection Act *(Zakon o varstvu osebnih podatkov;* Official Gazette of RS, nr. 94/2007), moreover, information regarding the websites the employee is visiting is personal data and as such is protected by the respective law. The employer is therefore only allowed to obtain information regarding which websites the employee has visited and collect such data

(i) with the employee's consent; or

(ii) on the basis of byelaws adopted by the employer in advance and only to extent as this is necessary for the implementation of the rights and obligations arising from the employment relationship. It is increasingly common for employers to have byelaws in place that either prohibit or restrict the use of the internet. From the perspective of personal data protection, a less invasive measure is to block certain websites. An employer intending to block certain websites should also adopt byelaws regulating use of the internet by employees and produce a list of blocked websites. Excessive use of the internet for private purposes during working hours, or its use for commercial or offensive purposes, could also be considered a breach of the employment contract and entitle an employer to terminate the contract.

Are there any specific requirements for doing so?

As explained above, there is no specific law regulating use of the internet for private purposes. As a result, this is often regulated by company byelaws. The employer has to consider provisions of the Slovenian Personal Data Protection Act *(Zakon o varstvu osebnih podatkov;* Official Gazette of RS, nr. 94/2007), however, as information about websites the employee is visiting is personal data, and personal data protection issues may arise as a result. See also Answer to previous Question.

Is the employee allowed to use his/her office e-mail account for private purposes?

Yes, if not forbidden by the employer on the basis of an internal rule or the employment contract.

Are there any specific requirements for doing so?

No. There is no specific law regulating the use of office e-mail for private use. This subject matter is often regulated by the byelaws of the employer as a result. However, the employer has to consider its employees' right to privacy and its own duty to respect and guarantee the employee's right to privacy. See also the answer to the next question below.

Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	No, the employer is not allowed to check either private e-mails ('gmail' or similar) or the employee's office e-mails. However, the employer may check office e-mail if this is specifically provided for in company byelaws or the employment contract, and subject to the following conditions: (i) that use of office e-mail is prohibited for private use in general; and (ii) that both the purpose and circumstances of the employer checking e-mails are provided for in advance in company byelaws or the employment contract (i.e. no random control of e-mails). The employee must be acquainted with this in advance.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	Yes. See answer to the previous question.
Data collection during the application process	
What information is the employer allowed to collect?	The employer may collect the following information from candidate employees: first name (names); surname; date of birth; residential address (address for correspondence); and education and employment history.
How long may data of this nature be stored?	Personal data may only be stored for as long as necessary to achieve the purpose for which they were collected. In the case of candidate employees, an employer should only process personal data until the recruitment process is complete.
Is the consent of the employee required?	A prospective employer is not required to gain an employee candidate's consent for storage of the data he collects in accordance with law. The employee or candidate must be informed of the following: (i) the purpose of collecting and storing the data; (ii) what personal data are to be processed; (iii) who will have access to this information, and under what circumstances; and (iv) how long the data are to be stored. The employer should regulate this in advance through a company byelaw.
GPS tracking	
Under what conditions can the employer use GPS tracking?	If GPS tracking is essential for the safety and security of the employee, and/or a legitimate interest is given on the part of the employer, then it is admissible. The employee should be informed that GPS tracking takes place. It is advisable to adopt company byelaws regarding the use of GPS tracking systems.
Use of video surveillance	
Is the employer allowed to use video surveillance?	Yes, if the requirements mentioned under the answer to the next question are met.
Are there any specific requirements for doing so?	It is advisable that the use of video surveillance be regulated in company byelaws. Generally visible video surveillance is allowed if necessary for the protection of a legitimate interest on the part of the employer. Hidden video surveillance is not allowed in principle. Under certain circumstances (e.g. theft of company property), the employer may have a legitimate interest in using hidden video surveillance, but this does not repair or justify the breach of data protection law, or the employer's exposure to sanctions. Employees must be notified in advance that the employer may be using (hidden) video surveillance. The works council has the right of consent with regard to company byelaws governing use of video surveillance.
Are there any situations/ locations where video surveillance is generally prohibited?	Video surveillance in non-public areas, such as dressing rooms, bathrooms, etc. is generally prohibited.

Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	There are no legal provisions on using information freely accessible over the internet, so it may be used by the employer.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	As with use of the internet, the employer is free to regulate the use of social media by means of company byelaws.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	The general rule applies that the collection of personal data should be both necessary and proportionate. Trade unions active at the place of work have a right of consent with regard to the rules and regulations governing systems for monitoring the performance of personnel.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Agreements with trade unions are possible in theory, but such agreements must be in line with the applicable legislation and general privacy principles.
To what extent can data collection, processing and use be justified by agreements with unions?	Please see above.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	No, the regulations of the law on data protection cannot be altered by consent of the employee. However, the employee's consent may justify the processing of data which otherwise would be a violation of data protection law.
If so, to what extent?	Not applicable.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	If there is no trade union operating, the employer should inform the works council of the adoption of company byelaws.
What kind of participation rights do unions have in relation to data protection?	If company byelaws are drafted, unions have a right to participate in the procedure. The employer must consult the union, but is not bound by their opinion.
Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	There is no specific regulation in law, so the general rules described below apply (See Answers to next two Questions below).

What are the requirements for data transfer to take place within a group?	Personal data of the employee may only be transferred in the following cases: — If the individual has consented to the transfer of his/her personal data; — If the transfer of the personal data is necessary for the fulfillment of the (employment) contract or the fulfilment of the rights arising out of that contract; — If the transfer of personal data is necessary to exercise legal powers, duties or liabilities of the public sector, and this does not interfere with the justified interests of the individual as provided for under the law. See also answer to the next question.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	Yes. If the data is to be transferred to a third country, the person wishing to transfer the data must obtain a decision from the Information Commissioner over whether the state in which the data is being sent ensures an adequate level of protection of the personal data. EU Member States are not considered third countries.

Duties of the employer connected with termination of an employment contract

Are there any duties relating to data protection connected with the termination of an employment contract?	No, there are no specific duties.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	In general, the information is to be permanently disposed of two years after the termination of the employment contract, unless another statutory retention period applies (e.g. for tax purposes).

Contacts

Contacts within own jurisdiction	Dunja Jandl **E** dunja.jandl@cms-rrh.com
Contacts within jurisdictions different from that mentioned in this list	Not applicable.

Spain



Group contact: Pedro Merry Monereo, Fernando Bazan

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	There is no law regulating use of the internet at work for private purposes. Spanish case law has established the main principles.The employer has the right to decide whether employees can use the internet for private purposes or not, and restrict access to the internet. Normally this use is regulated by internal policies and rules or works agreements. If use is not regulated by the employer, private use is admissible as long as it is kept within an ordinary and marginal limit.
Are there any specific requirements for doing so?	There are no specific statutory requirements concerning such use.
Is the employee allowed to use his/her office e-mail account for private purposes?	Unless instructed otherwise by the employer or the corresponding policy, he is allowed to do so in a normal use.These instructions can be contained in the employment contract, in a company´s policy and/or additionally, displayed as an on-screenmessage every time the user logs in.
Are there any specific requirements for doing so?	It would be neceasry to implement the non use of internet for personal purposes through policy the corresponding policy in the Company.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	The main criterion followed by Spanish courts is the "expectancy of privacy ". If the employee is instructed (policy) to use the company's computer for professional purposes only, he cannot expect any message to remain private. If there are no instructions, the personal use is moderate and the employee as a consequence, an in principle, those e-mails cannot be checked by the employer.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	Yes. The employer would put itself in a worse position by checking the computer due to the infrigment of the fundamental right, righ to the privacy during the rendering of services. Use of a computer control mechanism would be laid down in Article 20.3 of the Workers´ Statute, which establishes that the employer has the right to adopt any measures it considers appropriate to provide greater vigilance and control to ensure that workers carry out their obligations and work duties. He above-mentioned measures have several jurisprudential limitations; specifically, that constitutional doctrine requires that measures adopted by the employer comply with the principles of proportionality, necessity and suitability, otherwise it could be understood that this measure violates the employees´ right to personal privacy. To carry out the control as safely as possible, therefore, it would be necessary to inform workers of this mechanism of control before its implementation.

	In this sense, the following actions would be implemented: 1. Previously establish rules for the use of information technology (IT), including partial or total prohibitions of the computer; and 2. Inform employees that an IT control mechanism may be used. Case Law and instructions from the Data Protection Agency have provided extra regulation.
Data collection during the application process	
What information is the employer allowed to collect?	The employee must be informed of the collection necessary for the normal activities of the company to be carried out. The data collected must be adequate, relevant, not excessive, accurate and kept only for the period considered necessary. The employer shall inform the employee of his ARCO rights.
How long may data of this nature be stored?	No longer than necessary to fulfil the purpose of their collection.
Is the consent of the employee required?	Consent is not usually required, since the data processing is required for the employment relationship to be maintained. Despite this, the employer must inform the employee of what data are to be collected, and make clear the employee's rights of access, rectification, opposition and cancellation.
GPS tracking	
Under what conditions can the employer use GPS tracking?	Only if such tracking is proportional and necessary for the development of the professional activity. The employee that is going to be tracked must always be notified of the control.
Use of video surveillance	
Is the employer allowed to use video surveillance?	Yes.
Are there any specific requirements for doing so?	All camera installations must respect the principle of proportionality, which means taking into consideration other possibilities that could be less intrusive upon individual privacy. If there are no alternatives, then video surveillance can be implemented. Companies also have a duty to inform employees that the area is visibly monitored and made available to interested parties with information printed on the Data Protection Act. Finally, individuals or entities intending to create files of the video surveillance must give prior notice to the Data Protection Agency.
Are there any situations/ locations where video surveillance is generally prohibited?	It is generally prohibited in private areas such as toilets or private offices. Furthermore, video surveillance may not be used to control the work performance of employees.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	As the Supreme Court has not issued a ruling regarding this issue, the answer would be affirmative. The employer may check the candidate's profile on social networks, although it is subject to the same restrictions as those regarding the prohibition of collecting personal data, such as racial origin, political opinions, religion, health issues, etc.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	To the same extent as the use of the internet and e-mail. The regulation must be defined in the company's internal policies, and employees informed of the restrictions.

Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	No. It will depend on the company's internal policies, and must always be proportional.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Agreements with works councils should not change the rules on personal data processing.
To what extent can data collection, processing and use be justified by agreements with unions?	Collection and processing of employee data may be carried out without employee consent, inter alia, if foreseen by applicable legislation (e.g. employment law) or in a contract with the employee. However, it is difficult to see how an agreement between the employer and the union alone could justify such use of the data.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	No. Generally speaking, Spanish data protection legislation is imperative, and any agreement by employees to disregard it will be ineffectiveEmployees may consent to certain collection and uses of their data, however, although such consent must be "informed" (i.e. the employees must be made fully aware of the uses of their data before they consent) and freely given.
If so, to what extent?	Not applicable.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	In data protection issues, only the employee is entitled to exercise the ARCO rights concerning his/her personal data.
What kind of participation rights do unions have in relation to data protection?	They have a right to be informed and be heard in relation to any significant changes in working practices, which can extend to important changes in the use of employee data. The position is not always clear as to whether this obligation arises in any particular circumstances, but employee monitoring could be such a case. However, they cannot exercise ARCO rights as representatives of their members.
Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	Data transfer within a group is not regulated any differently than regular data transfer between an employer and a third party. In the event of such a transfer, all legal requirements need to be fulfilled, without exception.
What are the requirements for data transfer to take place within a group?	Transfer to a group company is a form of data processing, and the employer must comply with the relevant legal requirements.
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	Yes. A transfer of data to a country outside the EU requires that the other country ensures the same protection. Certain countries have been deemed adequate by the European Commission. The United States is not deemed to offer adequate protection, and data can only be transferred to US companies taking part in the Safe Harbor Program.

Duties of the employer connected with termination of an employment contract

Are there any duties relating to data protection connected with the termination of an employment contract?	Data will only be kept if considered necessary for the purpose for which it was initially collected. In this case, the information must be blocked by the employer.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	Five years

Contacts

Contacts within own jurisdiction	Pedro Merry **E** pedro.merry@cms-asl.com Blanca Cortés **E** blanca.cortes@cms-asl.com
Contacts within jurisdictions different from that mentioned in this list	

Switzerland



Group contact: Christian Gersbach, Philipp Dickenmann

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	The employer has the right to implement directives relating to use of the internet and to prohibit the use of the internet for private purposes. Such directives are recommended. If no directives are in place, the legal situation is not entirely clear, but from the employer's perspective it is certainly advisable to assume that (compared to private use of an office telephone), the employee is allowed to use the internet for private purposes to a limited extent.
Are there any specific requirements for doing so?	Use of the internet for private purposes is permitted unless the employer has implemented directives prohibiting such use. However, private use of the internet should not lead to a neglect of the employee's working duties.
Is the employee allowed to use his/her office e-mail account for private purposes?	The same principles apply as with use of the internet for private purposes.
Are there any specific requirements for doing so?	The same principles apply as with use of the internet for private purposes.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	The employer is only allowed to check the employee's e-mail under the following conditions: (i) That the employer is pursuing a justifiable interest which is higher than the employee's interest, and that checking the employee's e-mails is a proportionate means of pursuing such an interest (e.g. investigation of potential misconduct by the employee, if there is a valid suspicion that such misconduct has occurred and checking the e-mails is reasonably necessary for such investigation); (ii) In principle, it is recommended that the employee be informed in advance; (iii) The employer may not, in principle, check private e-mails; (iv) The number of people involved in viewing the e-mails should be kept to the minimum possible.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	No. Even if private e-mails are prohibited, the employer may not, in principle, review the private communications of an employee. In practice, however, such reviews are often conducted based on the argument that the employer does not have to expect that there will be private e-mails. If e-mails turn out to be private during such a review, they cannot be reviewed.

Data collection during the application process	
What information is the employer allowed to collect?	The employer may collect any data which is reasonably necessary to examine the applicant's aptitude for the envisaged employment. Questions relating to pregnancy, religion, political views or union membership are therefore only permissible in exceptional circumstances. Criminal records and excerpts from the debt enforcement register may be requested if relevant to the job, and to the extent necessary.
How long may data of this nature be stored?	Data of unsuccessful candidates must be returned and any copies thereof, as well as notes made by the interviewers, must be deleted after the recruitment process is complete. A longer storage period is possible if (cumulatively) the data may become relevant for future job openings, and the applicant agrees to such storage.
Is the consent of the employee required?	As a general rule, personal data may be collected and processed for the purposes indicated at the time of collection or evident based on the circumstances. If the employer collects sensitive data or personality profiles from third parties, he must inform the employee thereof. The consent of the employee is necessary if particularly sensitive data or personality profiles are disclosed to third parties.
GPS tracking	
Under what conditions can the employer use GPS tracking?	GPS tracking is only permissible, if (cumulatively): (i) The employee has been informed about the GPS tracking and the purposes thereof; (ii) The GPS tracking is reasonably necessary and proportionate to achieve a legitimate purpose (e.g. security concerns); (iii) The purpose of GPS tracking is not to survey the employee's behaviour. Constant and "real-time" GPS tracking will be much more difficult to justify than occasional or "ex-post" use of GPSdata. The Swiss Federal Supreme Court has adapted a rather restrictive view when determining whether GPS tracking is necessary to achieve a certain purpose.
Use of video surveillance	
Is the employer allowed to use video surveillance?	The employer is allowed to use video surveillance, if (cumulatively) (i) Surveillance of the employee's behaviour is not the primary purpose; (ii) The surveillance is reasonably necessary and a proportionate means for a legitimate interest (e.g. safety concerns or legal compliance), such interest being higher than the employee's interest in privacy; (iii) The surveillance is performed in the least invasive way in terms of the employee's privacy. The Federal Data Protection Commissioner recommends prior consultation of employees/employees' representatives, and the use of privacy filters.
Are there any specific requirements for doing so?	Employees must be informed about the use and purposes of CCTV, and areas in and around the buildings covered by CCTV should be marked accordingly with signs. Specific rules apply in case of an investigation of potential misconduct by an employee if there is a valid suspicion that such misconduct has occurred and video surveillance is reasonably necessary for such investigation. Footage must only be stored as long as necessary and kept secured against unauthorised access. Access to such data shall only be given to a very limited number of persons.
Are there any situations/ locations where video surveillance is generally prohibited?	It seems difficult to justify video surveillance of a break room for employees.

Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	The employer may only process data relating to the applicant's aptitude for the specific job or otherwise necessary for the employment relationship. Certain authors derive from this the rule that it is not permissible to use social media if the respective network normally concerns the employee's private life (e.g. Facebook), and not professional life (e.g. Xing). However, according to other authors, the consultation of even private social media is permitted, as the applicant can regulate the information available to third parties using the privacy settings of the media. In practice, employers often use private social media in their evaluation process as well.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	The employer has the right to implement directives concerning the use of social media during working hours, but he may only do so to a very limited extent regarding the use of social media during the employee's free time (e.g. use of company Facebook pages). This is usually contained in a code of conduct rather than issued as a directive.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	The following rules apply to efficiency controls: (i) The surveillance of the employee's behaviour must not be the primary purpose; (ii) The control system must be reasonably necessary and a proportionate means of monitoring the employee's efficiency; (iii) The efficiency control must be implemented in the least invasive way in terms of the employee's privacy; (iv) Employees must be informed about the system and its purpose.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Works councils do not exist in Switzerland. An employees' representation (if elected) does not have a particular function in relation to data protection.
To what extent can data collection, processing and use be justified by agreements with unions?	The employer may only collect, process and use the employee's data to the extent relevant for the employee's aptitude for a job and for processing of the employment. This rule is mandatory, and can only be altered by collective bargaining agreements if the alteration means an improvement in the employee's situation.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	No, the regulations of data protection law cannot be altered by consent of the employee. In certain cases, however, the employee's consent may justify the processing of data, which would otherwise be a violation of data protection law.
If so, to what extent?	Not applicable.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	The employees' representation (if elected) does not have a specific function with regard to data protection (the exception being surveillance measures which may have an impact on the employees' health; see above concerning the use of CCTV).
What kind of participation rights do unions have in relation to data protection?	None.

Data transfer within a group

Does data protection law provide for any special regulations relating to data transfer within a group?

As a general rule in Swiss data protection law, an affiliated company is treated in the same way as any other third party.

What are the requirements for data transfer to take place within a group?

A A transfer to an affiliate which processes data also for its own purposes is subject to the following conditions, *inter alia:*

(i) The respective data subjects must have been sufficiently notified of the processing by affiliates (or this was evident from the circumstances; in case of transfer of personality profiles or sensitive data, explicit consent is required from the employee);

(ii) Transfers to jurisdictions which do not have adequate data protection are only permissible if certain other safeguards are in place (e.g. binding corporate rules);

(iii) Regular transfers of personality profiles or sensitive data may trigger an obligation to register the data collection with the Swiss Federal Data Protection Commissioner.

B A transfer to an affiliate which only processes data for the transferring entity is subject to the following conditions:

(i) Data may only be processed in the manner permitted for the transferring entity;

(ii) Transfers to jurisdictions which do not have adequate data protection: see 'A', above;

(iii) The transferring entity ensures that the affiliate guarantees data security;

(iv) The transfer is not prohibited by a statutory or contractual duty of confidentiality.

Does it make a difference if the group company the data is to be transferred to is located within the EU or not?

EU countries are considered by the Swiss Federal Data Protection Commissioner to provide an adequate level of data protection. Cross-border data transfer safeguards are therefore not required for transfers within the EU.

Duties of the employer connected with termination of an employment contract

Are there any duties relating to data protection connected with the termination of an employment contract?

After termination of the employment, only those data may be kept by the employer that are still necessary. This is the case if a statutory document retention obligation is applicable, for example. Equally, documents may be kept which are necessary for a certificate of employment or job reference. Finally, data may be kept after termination if necessary for an ongoing or threatening legal dispute.

How long is an employer allowed/required to keep information concerning an employee who has left the company?

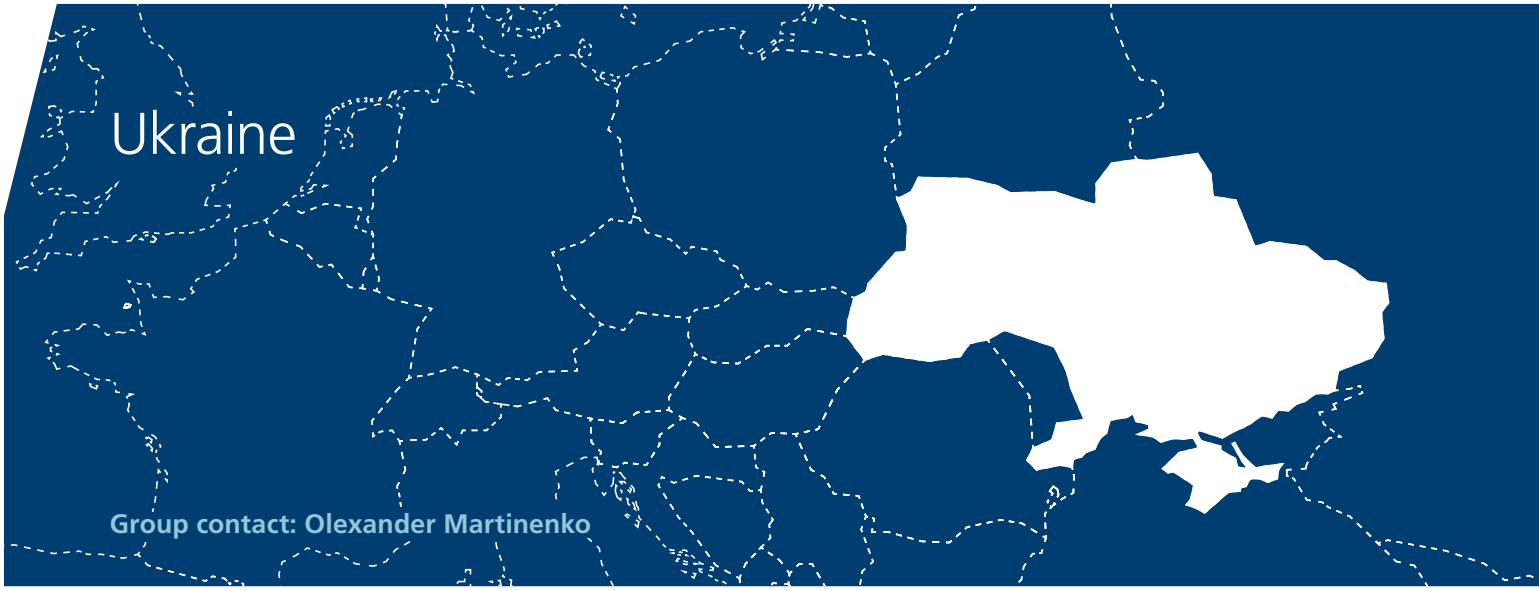
There is no absolute time limit. If data is no longer necessary, it has to be destroyed. The Swiss Federal Data Protection Commissioner requires that each category of data be looked at individually. As a rule, however, it will accept a period of five years. A longer timeframe applies if the data are subject to statutory document retention obligations (accounting documents, for example).

Contacts

Contacts within own jurisdiction

Christian Gersbach
E christian.gersbach@cms-veh.com
Philipp Dickenmann
E philipp.dickenmann@cms-veh.com
Markus Kaiser
E markus.kaiser@cms-veh.com

Contacts within jurisdictions different from that mentioned in this list



Ukraine

Group contact: Olexander Martinenko

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	There is no specific law or regulation covering internet use by employees. An employer may set up rules governing use of the internet by employees during working hours and/or use of employer's equipment (computers).
Are there any specific requirements for doing so?	No specific requirements. Under the general principle of Ukrainian labour law, an employee should dedicate his/her working hours and use employer's equipment only for due performance of his/her employment duties.
Is the employee allowed to use his/her office e-mail account for private purposes?	The law does not prohibit such use, so the issue depends entirely on the employer's instructions/regulations in this respect.
Are there any specific requirements for doing so?	No requirements are provided at legislative level. An employer may introduce such requirements.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	An employer is prohibited from checking the employee's private e-mail accounts. There is no specific regulation on employer's access to the work (corporate) e-mail accounts of their employees. However, such access must be in line with the personal data protection requirements applicable in Ukraine.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	The law is silent regarding this particular issue. In this case, however, an employer should set out clear requirements in its instructions/regulations for how corporate accounts may be used for private purposes (e.g. private e-mails should be always marked as "Private" or "Personal", to make them easy to identify).
Data collection during the application process	
What information is the employer allowed to collect?	Collection of an applicant's personal data by the employer must be in line with requirements of the Law on Personal Data Protection nr. 2297-VI, dated 1 June 2010. As a general rule, it is prohibited to collect or otherwise process any personal data relating to the racial or ethnic origin, or political opinions; religious or philosophical beliefs; political party or trade union membership; and sex life or health of the applicant. When it enters into the employment agreement, the employer is prohibited from requesting information about the employee's political party membership, nationality, origin or any other data/documents not required by law.

How long may data of this nature be stored?	An applicant's personal data may be stored for the defined period with the informed consent of the data subject (applicant), but for no longer than necessary for the lawful purpose of such data processing. If the applicant is not eventually employed, the law requires the company to keep some of his/her personal data (e.g. questionnaires, applications and CVs) for at least one year after the year in which handling of those papers has been completed.
Is the consent of the employee required?	No. Employment agreement with the employee is sufficient legal basis to process his/her personal data.
GPS tracking	
Under what conditions can the employer use GPS tracking?	Use of GPS tracking in an employment relationship is not specifically regulated by law. As a result, use of GPS tracking must be in line with requirements for personal data processing in general. Amongst other things, this implies that GPS tracking must be adequate and not excessive in light of the purpose of the personal data processing. The scope of the personal data to be collected using GPS tracking must be defined with the employee's consent.
Use of video surveillance	
Is the employer allowed to use video surveillance?	Yes, but only if the employee gives his/her consent to such video surveillance.
Are there any specific requirements for doing so?	No.
Are there any situations/ locations where video surveillance is generally prohibited?	This is not defined in the law. Use of video surveillance should not jeopardise the employee's honour and dignity, and should therefore not be carried out in toilets or similar private places.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	An employer is not prohibited from using social media as source of information concerning a job applicant. If such information is not in the public domain, however, then general rules for personal data processing apply.
Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	Yes. General rules of internet use (including social media) during working hours, and/or through the employer's equipment, will apply in this case (see comments in section entitled "Use of e-mail and the internet", above).
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	No.If efficiency control procedures involve processing of an employee's personal data, then general rules for personal data protection apply without exceptions or particularities.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	None. The applicable law does not provide works councils with any rights justifying the data collection process relating to an employee. Note: in Ukraine, a works council, unlike a trade union, is not a permanent establishment. A works council consists of representatives elected by all the employees to represent the workforce in certain matters (e.g. negotiating and approving collective bargaining agreements).

To what extent can data collection, processing and use be justified by agreements with unions?	None. Please see comment above.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	No.According to the law, the data subject's consent is required for most cases of personal data processing. The data subject's consent determines the main aspects of the data processing (its purpose, scope etc). Such consent does not overrule or alter the requirements of the law, however.
If so, to what extent?	Not applicable.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	None.
What kind of participation rights do unions have in relation to data protection?	None.
Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	No.General rules of personal data transfer to third parties apply equally to intra-group transfers.
What are the requirements for data transfer to take place within a group?	Data transfer within the group requires the consent of the employee (data subject).
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	No.In this case, the general requirements for cross-border data transfer apply. These requirements are: (i) that the data subject has consented to the transfer of his/her personal data outside Ukraine; and (ii) that an appropriate level of data protection can be ensured by the foreign party to which the data is being transferred.
Duties of the employer connected with termination of an employment contract	
Are there any duties relating to data protection connected with the termination of an employment contract?	No specific duties. If an employer continues processing the former employee's personal data, all the general personal data protection requirements of must be complied with.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	As a general rule, personal data should be kept for the period defined with the informed consent of the data subject (employee), but for no longer than necessary for the lawful purpose of such data processing. Ukrainian law also provides for minimum terms for storage by the employer of certain information/documents relating to former employees.

Contacts

Contacts within own jurisdiction

Olexander Martinenko
E olexander.martinenko@cms-cmck.com
Olga Belyakova
E olga.belyakova@cms-cmck.com
Nataliya Nakonechna
E nataliya.nakonechna@cms-cmck.com

Contacts within jurisdictions different from that mentioned in this list

United Kingdom



Group contact: Anthony Fincham

Use of e-mail and the internet	
Are employees allowed to use the internet for private purposes?	There is no law preventing employees from accessing the internet at work for private purposes, but it is very common for an employer to have a policy that either prohibits or regulates this. Such a policy would commonly involve prohibiting use of the internet for commercial or offensive purposes, and limiting time spent using the internet to minimal levels (e.g. during breaks or before/after working time).
Are there any specific requirements for doing so?	As explained above, the law does not prevent employee use of the internet in a work context, but employers normally have policies and procedures which regulate its use.
Is the employee allowed to use his/her office e-mail account for private purposes?	There is no law to prevent an employee from using a work e-mail account for private purposes, but employers will typically control this through their own policies and rules. Employers may ban use of the work e-mail for private purposes, or place restrictions on its use. Failure to comply with the policy is likely to be a disciplinary offence.
Are there any specific requirements for doing so?	This will depend on the employer's own policies and rules.
Is the employer allowed to check an employee's e-mails? If so, what requirements have to be set?	Monitoring e-mails is possible in the UK providing it is justified and there is an appropriate balance between allowing the worker to enjoy privacy in the workplace and the interests of the business. Where monitoring occurs there are data protection issues as it is a form of 'processing' and, under the Data Protection Act 1998 ("DPA"), the employer will have to comply with the eight 'data protection principles'. Most importantly, it must process information fairly and lawfully, which in practice means it must notify employees that such monitoring will take place. The employer must also satisfy data processing conditions, e.g. that the processing is necessary for a legitimate interest of the employer (such as preventing discrimination). The interception of communications is a complex area, and although employers can monitor communications for particular business reasons, legal advice should be sought in specific situations.
If so, does it make a difference if the employee is allowed to use the e-mail account for private purposes?	There is no specific legal distinction based on whether the employee is allowed to use the e-mail account for private purposes. In practice, however, those employees may have a greater expectation of privacy in relation to e-mails, so any monitoring should be particularly carefully explained. Employees are entitled to a degree of privacy at work, so any e-mails marked "private" or "personal" should only be monitored if there is a justifiable reason for doing so.

Data collection during the application process	
What information is the employer allowed to collect?	Only certain information is protected by the DPA. "Personal data", which is information relating to a living person (such as his/her name, salary, bank account details, etc.) is protected but in practice can usually be collected by employers. "Sensitive personal data", which is particular information about the data subject (such as racial/ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or information about the employee's sexual life) is more difficult to collect, as such processing must satisfy one of a very limited set of conditions, and sensitive personal data should therefore only be collected to the extent absolutely necessary. The data protection principles govern the way the data should be collected/processed (e.g. the data collected must be adequate, relevant and not excessive, accurate, not kept longer than needed, and stored securely). The first principle requires that data is processed fairly and lawfully. To comply with this principle, employers must be able to rely on one of the conditions for processing personal data (e.g. the employee must have given consent, or the processing is necessary for the legitimate interests of the employer).
How long may data of this nature be stored?	No longer than is necessary. Guidance has been issued by the Information Commissioner (the UK regulator in respect of data protection); for example, information obtained from a vetting exercise should be destroyed as soon as possible, or within six months at the latest.
Is the consent of the employee required?	Consent is one of the 'processing conditions' that can be used to justify processing personal data. It is common for consent to be sought, but consent must be specific, informed and freely given. It is arguable that it is not always possible for employees to give consent freely in an employee/employer relationship. Therefore, best practice is to ensure that an alternative processing condition is satisfied, e.g. that the processing is necessary for the purposes of the legitimate interests of the employer (the data controller).
GPS tracking	
Under what conditions can the employer use GPS tracking?	GPS tracking is a form of monitoring, and results in the collection of personal data. It is therefore covered by the DPA principles. As this type of monitoring is intrusive, the employer would need to be clear that it had a strong justification for requiring this.
Use of video surveillance	
Is the employer allowed to use video surveillance?	The Information Commissioner has issued specific guidance in relation to CCTV (closed-circuit television). In principle, this can be lawful provided the benefits justify any adverse impact.
Are there any specific requirements for doing so?	The Information Commissioner guidance covers video surveillance. In addition to normal DPA principles, it states that all workers (and visitors) should normally be aware of its use, unless covert monitoring can be justified as part of a specific investigation, e.g. where criminal activity is suspected and the use will be limited.
Are there any situations/ locations where video surveillance is generally prohibited?	The Information Commissioner guidance states that surveillance should not take place in areas that workers would genuinely and reasonably expect to be private, such as toilets or private offices.
Social media	
Is the employer allowed to use social media as a source of information concerning a job applicant?	Employers can use social media as a source of information. However, this approach can create legal issues. For example, if an employer appears to base its recruitment decisions on (sensitive) personal information found on a social media site, this could lead to a discrimination claim. The employer must, of course, comply with the DPA in respect of the processing of personal data collected via social media.

Is it possible for the employer to regulate the use of social media – in relation to the content and scope of that use – by employees?	It is possible to regulate this through an appropriate policy. The absence of a clear policy makes it very difficult to regulate the use of social media.
Efficiency control	
Does data protection law provide for any regulations relating to controls on the efficiency of employees?	There is no specific data protection law relating to efficiency controls, but various forms of controlling and monitoring efficiency may have data protection implications.
Justification of data collection, processing and use with the help of the works council/unions	
To what extent can data collection, processing and use be justified by agreements with works councils?	Works councils are not common in the UK. However, an agreement with a works council that processing is reasonable or required, etc. may be helpful evidence in supporting the employer's justification of the processing. However, it is not enough in itself to permit the processing of personal data.
To what extent can data collection, processing and use be justified by agreements with unions?	Any data processing (including collection and use) must be justified by reference to one or more of the processing conditions in the DPA (and one or more sensitive processing conditions in the case of sensitive personal data). Agreement with a trade union that processing is reasonable or required, etc. may be helpful evidence in supporting the employer's given justification, but it is not enough in itself to permit the processing of personal data.
Justification by consent of the employee	
Can the regulations of data protection law be altered by consent of the employee?	Consent does not alter the data protection regulations, but is one of the conditions upon which employers can rely in order to process personal data of its employees. However, a blanket consent provision in an employment contract is not necessarily sufficient to cover all the laws on data protection. Please see comments below.
If so, to what extent?	Consent must be appropriate to the particular circumstances, specific, informed and freely given. However, consent is only one of the conditions for processing set out in the DPA, and is not always necessary if another condition is complied with, though employers often regard this as the "safest option". Where 'sensitive personal data' (race/ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical/mental health, sexual life) is to be processed, an additional processing condition must be satisfied from a separate list in the DPA, and often explicit consent is required for this purpose.
Participation rights of the works council and unions	
What kind of participation rights do works councils have relating to data protection?	No automatic rights.
What kind of participation rights do unions have in relation to data protection?	No automatic rights.
Data transfer within a group	
Does data protection law provide for any special regulations relating to data transfer within a group?	There is no specific regulation relating to data transfer within a group. However, the information given to employees about any processing should make clear how that information will be used and shared, and this includes explaining if it will be shared with group companies.

What are the requirements for data transfer to take place within a group?	Transfer to a group company is a form of processing, so the employer must be able to comply with the normal DPA requirements, including being able to satisfy a processing condition (and sensitive data processing condition if applicable).
Does it make a difference if the group company the data is to be transferred to is located within the EU or not?	Yes. Where there is to be a transfer of data to a country outside the European Economic Area, the eighth data protection principle requires that this can only be done where that other country ensures adequate protection in relation to data protection. Certain countries have been deemed adequate by the European Commission (e.g. Switzerland, Argentina). The United States is not deemed to have adequate protection but has in place the Safe Harbor scheme, which is deemed sufficient, if the relevant company has signed up to it. In other cases, where adequacy is in doubt, employers can use contracts, including the European Commission-approved model contractual clauses, or get Binding Corporate Rules approved by the Information Commissioner.

Duties of the employer connected with termination of an employment contract

Are there any duties relating to data protection connected with the termination of an employment contract?	Termination of the employment relationship raises the issue of whether the employer may continue to hold and process personal data, and for how long.
How long is an employer allowed/required to keep information concerning an employee who has left the company?	Businesses must ensure they do not retain personal data of former employees once there is no longer a legitimate business need or legal requirement to do so. This should then be securely disposed of, by shredding, for example. There is no specific timescale in the DPA, as it is recognised that there are a number of varying reasons and circumstances that could apply.

Contacts

Contacts within own jurisdiction	Anthony Fincham **E** anthony.fincham@cms-cmck.com
Contacts within jurisdictions different from that mentioned in this list	John Armstrong **E** john.armstrong@cms-cmck.com

Contacts

Albania
Tirana
CMS Adonnino Ascoli & Cavasola Scamoni Sh.p.k.
T +355 4 430 2123
E marco.lacaita@cms-aacs.com

Algeria
Algiers
CMS Bureau Francis Lefebvre
T +213 2 137 0707
E samir.sayah@cms-bfl.com

Austria
Vienna
CMS Reich-Rohrwig Hainz Rechtsanwälte GmbH
T +43 1 40443 0
E bernhard.hainz@cms-rrh.com

Belgium
Antwerp
CMS DeBacker
T +32 3 20601 40
E jef.degrauwe@cms-db.com

Brussels
CMS DeBacker
T +32 2 74369 00
E michael.deleersnyder@cms-db.com

Bosnia and Herzegovina
Sarajevo
Attorney at law in cooperation with CMS Reich-Rohrwig Hainz d.o.o.
T +387 33 2964 08
E nedzida.salihovic-whalen@cms-rrh.com

Brazil
Rio de Janeiro
CMS Cameron McKenna
T +44 20 7367 2000
E ted.rhodes@cms-cmck.com

Bulgaria
Sofia
CMS Cameron McKenna LLP – Bulgaria Branch/Duncan Weston
T +359 2 92199 10
E david.butts@cms-cmck.com

Sofia
Pavlov and Partners Law Firm in cooperation with CMS Reich-Rohrwig Hainz
T +359 2 447 1350
E gentscho.pavlov@cms-rrh.com

China
Beijing
CMS, China
T +86 10 8527 0287
E nick.beckett@cms-cmck.com

Shanghai
CMS, China
T +86 21 6289 6363
E jeanette.yu@cmslegal.cn

Croatia
Zagreb
CMS Zagreb
T +385 1 4825 600
E gregor.famira@cms-rrh.com

Czech Republic
Prague
CMS Cameron McKenna v.o.s.
T +420 2 96798 111
E tomas.matejovsky@cms-cmck.com

France
Lyon
CMS Bureau Francis Lefebvre Lyon
T +33 4 7895 4799
E courrier@lyon.cms-bfl.com

Paris
CMS Bureau Francis Lefebvre
T +33 1 4738 5500
E info@cms-bfl.com

Germany
Berlin
CMS Hasche Sigle
T +49 30 20360 0
E berlin@cms-hs.com

Cologne
CMS Hasche Sigle
T +49 221 7716 0
E koeln@cms-hs.com

Duesseldorf
CMS Hasche Sigle
T +49 211 4934 0
E duesseldorf@cms-hs.com

Dresden
CMS Hasche Sigle
T +49 351 8264 40
E dresden@cms-hs.com

Frankfurt
CMS Hasche Sigle
T +49 69 71701 0
E frankfurt@cms-hs.com

Hamburg
CMS Hasche Sigle
T +49 40 37630 0
E hamburg@cms-hs.com

Leipzig
CMS Hasche Sigle
T +49 341 21672 0
E leipzig@cms-hs.com

Munich
CMS Hasche Sigle
T +49 89 23807 0
E muenchen@cms-hs.com

Stuttgart
CMS Hasche Sigle
T +49 711 9764 0
E stuttgart@cms-hs.com

Hungary
Budapest
Ormai és Társai
CMS Cameron McKenna LLP
T +36 1 48348 00
E gabriella.ormai@cms-cmck.com

Italy
Rome
CMS Adonnino Ascoli & Cavasola Scamoni
T +39 06 4781 51
E fabrizio.spagnolo@cms-aacs.com

Luxembourg
Luxembourg
CMS DeBacker Luxembourg
T +352 26 2753 1
E julien.leclere@cms-dblux.com

Morocco
Casablanca
CMS Bureau Francis Lefebvre
T +212 522 2286 86
E marc.veuillot@cms-bfl.com

The Netherlands
Amsterdam
CMS Derks Star Busmann
T +31 20 3016 301
E katja.vankranenburg@cms-dsb.com

Utrecht
CMS Derks Star Busmann
T +31 30 2121 111
E robertjan.dil@cms-dsb.com

Poland
Warsaw
CMS Cameron McKenna
Dariusz Greszta Spólka Komandytowa
T +48 22 520 5555
E katarzyna.dulewicz@cms-cmck.com

Portugal
Lisbon
CMS Rui Pena & Arnaut
T +351 210 958 100
E susana.afonso@cms-rpa.com

Romania
Bucharest
CMS Cameron McKenna SCA
T +40 21 4073 800
E loredana.ralea@cms-cmck.com

Russia
Moscow
CMS, Russia
T +7 495 786 4000
E sergey.yuryev@cmslegal.ru

E leonid.zubarev@cmslegal.ru

Serbia
Belgrade
CMS Reich-Rohrwig Hainz d.o.o.
T +381 11 3208 900
E radivoje.petrikic@cms-rrh.com

Slovakia
Bratislava
Ružička Csekes s.r.o.
in association with members of CMS
T +421 2 3233 3444
E peter.simo@cms-rrh.com

Slovenia
Ljubljana
CMS Reich-Rohrwig Hainz
T +386 1 62052 10
E ales.lunder@cms-rrh.com

Spain
Barcelona
CMS Albiñana & Suárez de Lezo
T +34 91 4519 300
E fernando.bazan@cms-asl.com

Madrid
CMS Albiñana & Suárez de Lezo
T +34 91 4519 300
E fernando.bazan@cms-asl.com

Seville
CMS Albiñana & Suárez de Lezo
T +34 95 4286 102
E fernando.bazan@cms-asl.com

Switzerland
Zurich
CMS von Erlach Henrici
T +41 44 2851 111
E philipp.dickenmann@cms-veh.com

Turkey
Turkish Department Vienna
CMS Reich-Rohrwig Hainz
Rechtsanwälte GmbH
T +43 1 40443 0
E doene.yalcin@cms-rrh.com

Ukraine
Kyiv
CMS Cameron McKenna LLC
T +380 44 39133 77
E olexander.martinenko@cms-cmck.com

Kyiv
CMS Reich-Rohrwig Hainz TOV
T +380 44 50335 46
E johannes.trenkwalder@cms-rrh.com

United Kingdom
London
CMS Cameron McKenna LLP
T +44 20 7367 3000

Employment
E anthony.fincham@cms-cmck.com

Pensions
E mark.atkinson@cms-cmck.com

CMS Legal Services EEIG is a European Economic Interest Grouping that coordinates an organisation of independent member firms. CMS Legal Services EEIG provides no client services. Such services are solely provided by the member firms in their respective jurisdictions. In certain circumstances, CMS is used as a brand or business name of, or to refer to, some or all of the member firms or their offices. CMS Legal Services EEIG and its member firms are legally distinct and separate entities. They do not have, and nothing contained herein shall be construed to place these entities in, the relationship of parents, subsidiaries, agents, partners or joint ventures. No member firm has any authority (actual, apparent, implied or otherwise) to bind CMS Legal Services EEIG or any other member firm in any manner whatsoever.

CMS member firms are:
CMS Adonnino Ascoli & Cavasola Scamoni (Italy);
CMS Albiñana & Suárez de Lezo (Spain);
CMS Bureau Francis Lefebvre S.E.L.A.F.A. (France);
CMS Cameron McKenna LLP (UK);
CMS DeBacker SCRL/CVBA (Belgium);
CMS Derks Star Busmann N.V. (The Netherlands);
CMS von Erlach Henrici Ltd (Switzerland);
CMS Hasche Sigle, Partnerschaft von Rechtsanwälten und Steuerberatern (Germany);
CMS Reich-Rohrwig Hainz Rechtsanwälte GmbH (Austria) and
CMS Rui Pena, Arnaut & Associados RL (Portugal).

CMS offices and associated offices:
Aberdeen, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Berlin, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dresden, Dubai, Duesseldorf, Edinburgh, Frankfurt, Hamburg, Kyiv, Leipzig, Lisbon, Ljubljana, London, Luxembourg, Lyon, Madrid, Milan, Moscow, Munich, Paris, Prague, Rio de Janeiro, Rome, Sarajevo, Seville, Shanghai, Sofia, Strasbourg, Stuttgart, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

www.cmslegal.com

© CMS Legal Services EEIG (July 2013)