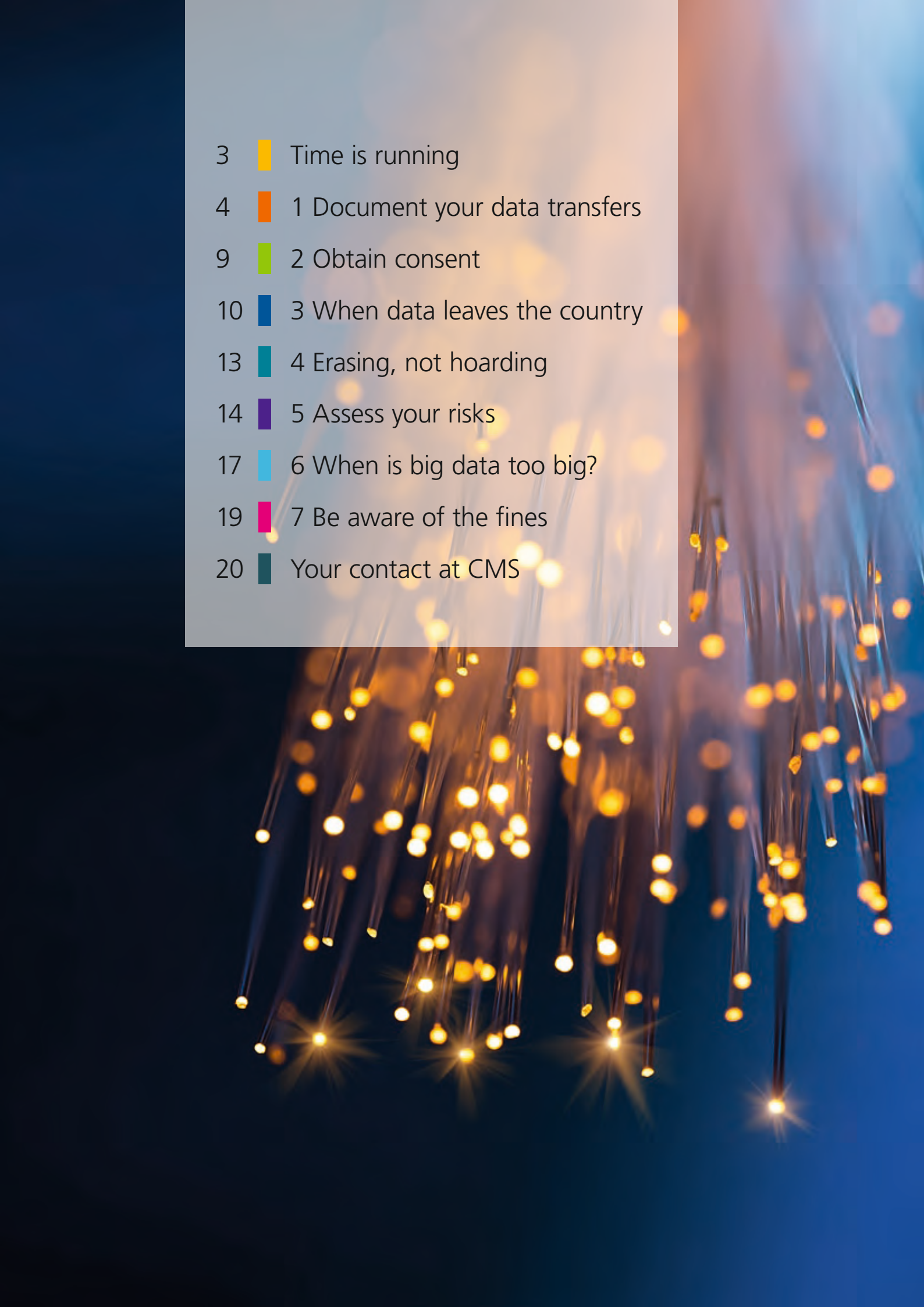
CMS
law·tax·future

How to be prepared for the GDPR in 7 steps

How to prepare yourself and your business for the EU's new General Data Protection Regulation (GDPR).
Which hefty fines you will have to be aware of in the future; and why also SMEs will have to take compliance seriously.



Time is running

In May 2018, the EU's new General Data Protection Regulation (GDPR) will enter into force. Violations can incur fines of up to EUR 20 million or 4% of the company's turnover. So companies – both global enterprises and SMEs – have to start with their preparations now.

The digitalization has fundamentally changed many business models: manufacturing enterprises can directly deliver goods to final customers via an online shop, spare parts can be ordered in the supplier's online shop, payroll accounting can be outsourced to an external service provider. And, as is widely known, the new oil that keeps such processes running is personal data. For the EU this was reason enough to define a strict framework for collecting and transferring data.

The new General Data Protection Regulation (GDPR), which enters into force on 25 May 2018, intends to protect the rights of data subjects. It also seeks to ensure uniform standards of data protection across the EU and to simplify cross-border data exchange within the EU. Yet initially companies will face a more complex situation.

Intensifying data protection efforts

The new GDPR entails a lot of changes particularly for companies: data controllers, for instance, will be responsible to take measures that ensure safety and data protection when they process data. Managing directors, decision makers, marketing and HR heads and also other staff members within the company will have to take a closer look at data protection than in the past.

So you are well advised to take the necessary measures to prepare for the GDPR as your duties will increase once it enters into force: for example, companies will be required to disclose which personal data they collect for what purposes and also how they handle the erasure of data. This also concerns their relationship with data processors, i.e., service providers abroad commissioned to process data on behalf of the data controller.

The significant increase in the amount of fines imposed by the EU is a further good reason to be prepared: while in the past, data protection violations have been sanctioned with penalties of not more than thousands of EUR (depending on the national data protections laws of each EU Member country), the GDPR stipulates fines of up to EUR 20 million or up to 4% of the total worldwide annual turnover. In other words: fines that really hurt and that show how important it is for companies to ensure compliance with the GDPR in due time.

Almost all companies are concerned

The GDPR concerns – albeit in varying degrees – virtually all companies. Even many SMEs, which have been paying little attention to the topic of data protection up to now, collect customer or employee data. This means that they will also have to be able to present a record of processing activities in the future. The efforts and IT resources that companies will have to invest to implement such records naturally depend on the risks for the rights of data subjects in the respective company. A company processing health-related data, for instance, will require significantly more resources than other enterprises.

Using the remaining time to get prepared

The following **seven steps** describe what exactly you have to do to be perfectly prepared for the new Regulation. While for some companies all seven steps will apply, others will find that some steps do not concern them. But what is true for all of them: there is not much time left until the GDPR enters into force. And this time should be used to implement the necessary changes in your organization.

1 Document your data transfers

In a first step, you have to assess the status quo: find out which data is processed within your organisation. This is the only way to prevent mistakes when establishing a record of processing activities.

On 25 May 2018, the transition period for the (full) implementation of the GDPR ends and compliance with its stipulations becomes legally mandatory. This also means that from that day on data processing operations carried out by data controllers must satisfy the provisions laid out in the GDPR. The first challenge to be tackled when creating a compliance system heeding all data protection provisions is establishing a record of processing activities. Such records of processing activities are intended to enable the data protection authority to review the respective data processing operations. This means that such records must contain all data processing operations carried out in your company. So as a first step, you must identify all data processing operations, document them in a written or electronic format and finally make them available in a concise way in the record of processing activities.

Requirements your company must meet at a glance

Dynamic records
The record of processing activities is "dynamic", i.e., all identified or defined data processing operations shall be reviewed on a regular basis with regard to the question whether the processes still run the same way as they initially have been determined and documented. If processing activities change due to changes in the company's demands, this has to be mirrored in the record of processing activities. For this reason, the responsible contact person in the respective department should be contacted on a regular basis, e.g., once a year.

History
Your company is required to prove (at any time) that personal data has been processed in a lawful manner (at all times). This follows that the record of processing activities shall contain a history that has to be kept updated in order to prove compliance with the GDPR, also for a past period of time.

Contact persons
With regard to contact persons, the GDPR only stipulates that the data controller, its representative and, where applicable, the data protection officers shall be named as contact persons. However, it will facilitate the work of a national Data Protection Authority and reduce the amount of follow-up questions in the course of an audit, if, additionally to the information explicitly required by the GDPR, the record names the persons responsible for the respective processing activities (e.g. name and contact details of the head of HR, head of IT, etc.).

Data mapping: determining the data

Use the following questions to get an overview of the data processing operations performed in your company and to be able to establish an exhaustive and up-to-date record of processing activities. These questions will help you identify the essential components of the said record.

Whose personal data do you need?
Depending on the company you work for and your department, you might come across data of applicants, employees, suppliers, shippers, consumers, prospective and existing customers, contact persons at companies you cooperate with, third parties acting as facilitators for your business relationships with other companies, the company's bodies (and their members) and other function holders of legal entities, etc.

Important questions:

Who?
Assess from which natural persons you obtain data.

Why?
Identify the purposes for which you need personal data.

Which?
Closely look at which data categories you collect (including data you might collect unintentionally) and use.

How?
You also have to think about how you obtain the data.

For how long?
Finally, establish rules on how long you store data. In order to gain an overview of your data processing activities, enabling you to establish a comprehensive and up-to-date record of processing activities, you have to ask the following questions:

For what purpose do you need the data?
First, think about why you need the personal data. Do you, for example, work in the logistics or accounting department and need the data for maintaining business relationships with customers? Or do you work in the HR department and need data for payroll accounting as well as for fulfilling record-keeping and reporting requirements and obligations to provide information? Or are you part of the marketing department of your company and use your company's or purchased customer and prospect data to initiate business with regard to your range of products and services?

What data do you use?
Depending on the natural persons from whom you collect data and the purpose of the collection, various kinds of data may be included. If you, for example, collect data for managing customer satisfaction or business relationships with customers, you will most probably deal with customer data including the name of the customer, the name of the contact person acting for the customer, the internal customer number, address data (e.g. place of establishment), contact data (email address, fax number, telephone number), etc. If you work in the HR department, you will mostly deal with employee or applicant data concerning, for example, personal data (name, address, date of birth) or the employment relationship (full-time/part-time, salary, length of service, supervisor, responsibilities within the company).

How do you collect the data?
Finally, you will have to deal with the question of how to obtain the data from the data subjects. Does your company, for example, operate an online shop where the customer can buy goods online? In that case, you will most probably need the customer data in order to ship the goods to the customer's place. Otherwise, you will not be able to meet the obligations arising from the contract with the customer. Or do you work in the HR department and need data from new employees in order to report the employment status to the social insurance provider? In such a case, data is necessary for you to fulfill the company's legal obligations.

Our parent company is located in the USA. Is it permissible to transfer our employee's data to them?

In addition to clearly defining the purpose (in the case of global enterprises, this is often the matrix structure), the international data transfer has to be covered by a certification according to the EU-US Privacy Shield framework or, e.g., the EU Standard Contractual Clauses.

To what extent is it permissible to use cloud services?

In addition to other prerequisites to be met, particularly the necessary contractual stipulations for outsourcing (usually the EU Standard Contractual Clauses) must be in place.

I have been sending out newsletters for many years. Am I allowed to continue to do that in the future?

Yes, if the recipients are your customers or if the data processing operation is based on a valid consent and a comprehensive Privacy Policy.

2 Obtain consent

The sending of promotional emails or newsletters could be a stumbling block. Be aware that it is illegal to send promotional emails to data subjects with whom you do not have a business relationship unless you have obtained their valid consent.

Sending promotional messages is generally not permissible if those messages are being sent without the consent of the recipient or, if the number of recipients exceeds 50 and the sender does not maintain a business relationship with the recipients. Explicit consent is not required, if

— the recipient has disclosed his or her address to the sender in the course of a business process; and
— the sender solely uses the contact address for advertising further products and services he or she offers; and
— the recipient has the option to decline at any time in the course of the communication process and free of charge to receive further promotional emails.

Identify yourself

Do not forget to use the company's official email address and place a clearly visible "unsubscribe" link in your promotional email to allow the recipient to opt out from receiving further messages at any time. Also keep in mind that every newsletter or promotional email has to be marked as such, for example, by clearly indicating this in the subject line. Also remember that the sender has to be clearly identifiable at any time with the help of a legal notice on the website and an email signature containing further contact information.

The dilemma of "yes, I do"
In practice, data subjects usually give consent to receiving newsletters or promotional emails via an opt-in. Opt-in means that the data subjects give their consent to receive emails on a regular basis (e.g. newsletters) in advance. Also, bear in mind that the checkbox must not be pre-selected. A best-practice solution is to ask users to click a checkbox accompanied by a text that could be drafted as follows:

"I hereby grant the XY company permission to process my data [i.e., ... (exact and exhaustive list) ...] pursuant to the Privacy Policy [insert URL to the Privacy Policy] for the purpose of receiving promotional materials for the XY products of the company. This permission granted to XY GmbH is voluntary and can be revoked at any time via email to newsletter@XYGmbH.com."

Please note that the Privacy Policy must also comply with the stipulations of the GDPR.

3 When data leaves the country

Is your parent company located abroad or have you, for example, outsourced IT processes to a service provider outside of the EU or the EEA? If you answered yes to any of these questions, there are several things to keep in mind in the future:

Where do you transfer personal data?

In today's globalised business world where companies merge worldwide and save costs by outsourcing certain business processes (such as IT services or payroll accounting), international data transfers are an integral part of daily business. When establishing a record of processing activities, you must also indicate to where you transfer the personal data and with whom you share the personal data you have collected. Your company remains the responsible data controller for the data processing operation regardless of the fact whether or not you transfer data to a recipient in another country. This means that your company, being the data controller transferring the data, shall ensure that the data subjects' personal data categories are adequately protected in the course of the transfer. The following text will show you how difficult it can be to map data transfers abroad.

Searching for and finding points of reference

In a first step, look for points of reference in the existing documentation: is there, e.g., a database stating data transfers to certain locations? Does your company rely on a so-called cloud solution or does it save the data locally? Are you a large corporation with subsidiaries or branches outside of the country where your company is located? Do you cooperate with suppliers in other countries? Does an external payroll provider handle your company's payroll accounting and do your employees receive electronic payslips? Is your parent company, that is located in a different country, responsible for the IT maintenance of your company's computers?

Integrate the responsible people from an early stage on

Keep in mind that data privacy is a topic that concerns everybody in the company: for this reason, it is a good idea to involve the HR, Marketing, IT and other departments in your company in all steps you are taking right from the start. Schedule meetings with these departments on a regular basis in order to reflect on the on-going process and involve data privacy experts at an early stage of the process. Consider making a good investment by seeking professional advice.

What you should know

Also under the GDPR, data transfers to so-called third countries remain a complex issue. Third countries are those that belong to neither the European Union nor the European Economic Area (Iceland, Norway and Liechtenstein). Examples include China, Russia, India and the USA.

But let us start with the good news: once you have identified all parties to which you send data and these are located in EU or EEA member states, the data transfer is legitimate provided that the recipient has a legitimate interest to the transfer, too. In case you use a data processor, a respective contractual agreement has to be in place. This also applies to data transfers to countries with an adequate level of data protection (which has been determined by the EU). These include Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

Attention when you transfer personal data to the USA!

Generally, the data protection level in the USA is not considered being adequate. In order to still facilitate data transfers for European business partners, the EU and USA have entered into the "EU-US Privacy Shield" framework. To make use of this arrangement, the respective US-based company has to register itself to a specific list and self-certify itself. Prior to transferring data to this US company, your company only has to check whether the recipient is registered in the list of the US Department of Commerce and verify that the certification has not yet expired.

If the recipient does not fit in any of the above mentioned categories, your company, being the data controller, still has to ensure that the recipient provides an adequate level of data protection. In such a case, it is strongly recommended to use the Standard Contractual Clauses drafted by the EU. Such a contract can, in principle, be used without first consulting your national Data Protection Authority provided that no changes are made to its provisions. If individual clauses have been changed by the contracting parties, the contract has to be approved by the Data Protection Authority. Please keep in mind that data transfers that occur outside the scope of commissioned data processing operations always require a legitimate interest in the data in order to be considered legitimate.

It is permissible if...

1.

It is permissible to send data abroad if the recipient is located in the EU or the EEA including Norway, Iceland and Liechtenstein and has a legitimate interest tothe data transfer.

2.

It is also permissible to transfer data to countries providing an adequate level of data protection according to the European Commission. This list currently includes Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. Transferring data to the United States is only included in this stipulation if the recipient has obtained a certification according to the EU-US Privacy Shield framework.

3.

All other international data transfers are only permissible if certain exceptions apply, such as the use of the EU Standard Contractual Clauses or, if the data subjects have given their consent to the transfer.

An external newsletter provider handles our mailings. Will we be able to continue this cooperation in the future?

Yes, provided that the service provider is a data processor and a respective contract is in place. Additionally, you have to inform the data subjects in your Privacy Policy that you are commissioning third parties.

4 Erasing, not hoarding

Data subjects can also revoke their consent to the use of their data. The GDPR thus stipulates the "right to be forgotten": find out how you can keep an eye on the timely erasure of data

When establishing a record of processing activities, it shall be documented which personal data are processed by using which automated procedure and which concrete measures are taken in order to protect the data. This includes defining the periods during which the personal data are stored and after which they have to be erased. Such periods will not only be a crucial point of interest for the Data Protection Authority, but they also serve self-monitoring purposes.

How do you realise the erasure of data in practical terms and which periods apply?

The GDPR does not define specific periods after which the data has to be erased. As a result, many companies simply state that they will erase data once they are no longer needed and neglect to state specific periods during which data are saved. Such an approach not only makes an external audit more difficult, but it could give rise to the suspicion that the erasure of personal data has not been given due consideration.

A good data management solution includes an archive function, deadline reminders and delete functions on the data level. Your company should make sure that storage periods are assigned to data categories and that these are regularly reviewed by the competent department, which also deletes those data categories for which the storage period has expired.

Therefore, it can be a good idea for the contact persons of the various departments to use respective functions in their electronic calendars that issue a reminder whenever such a review is due.

Attention!

With "the right to be forgotten", the GDPR grants data subjects who have consented to their data being processed the right to have their data erased the moment he or she withdraws the consent. In such a case, a company not only has to stop sending the data subject e.g., promotional emails, but it is also obliged to inform third parties (to whom the data has been transferred) of the data subject's order to delete the data. Such data must then be erased.

5 Assess your risks

The GDPR states that companies are responsible to assess whether their data processing operations could impose a risk to data subjects. If this is the case, you must perform a detailed privacy impact assessment before commencing any data processing activities.

The GDPR orders companies to perform a privacy impact assessment ("PIA") before initiating data applications (that bear a risk for data subjects). Companies must first assess whether their data processing operations will potentially impose a risk to the rights and liberties of data subjects. If there is a high risk, they must then perform a detailed PIA. The most challenging part of a PIA will likely be to assess whether there is a high risk in one's company. In this context, the GDPR focuses on the perspective of the data subject, i.e. the question whether the rights and liberties of the individual could be affected (in practice, such curtailments of personal rights of the data subject are called "privacy impact").

In the course of data mapping, all departments in your company should first perform an assessment of said impact and thereby assess risks for the data subjects. The second step should be to describe the processing operations and the measures to be taken ("What exactly do I do and what can I do to reduce the risk?"). The GDPR leaves it up to the data controllers to decide on how they want to realise this process.

In practice, especially companies that use new technologies (such as tracking tools), work with special data categories (e.g., health-related data, crime-related data, etc.) or process data according to a so-called blacklist (a list of particularly high-risk types of data processing that will be published by the national Data Protection Authority in the future) will have to perform PIAs.

CMS is developing a

GDPR Helptool

The CMS GDPR Helptool is an electronic questionnaire where you can fill in details about your data processing operations. This information will then be processed into a written report by a CMS specialist, enabling you to assess the risks in your organization.

Privacy by default and privacy by design

These two buzzwords refer to technical concepts described in the GDPR that your company will not get around heeding and implementing: data protection as a default setting ("**privacy by default**") and data protection through technical means ("**privacy by design**"). This means that IT systems have to be configured in a way that the programming has already greatly reduced the possibility of illegitimate data processing operations. For example, checkboxes must not be pre-selected in a way that pushes users to consent.

Establishing a record of processing activities is a crucial prerequisite for being able to take adequate technical and organisational measures to provide for privacy by default and privacy by design. This is because once your company has internalised the requirements to be met to legitimately process personal data, it is easier to decide which measures have to be taken for these two privacy settings.

— According to the principle of **privacy by default**, your company's website should offer **suitable privacy settings** to users. If, for instance, your website has an online marketing section including an option to register for an online account, the user must be given the possibility to view the consent he or she has given and to revoke it at any time. In the end, a system has to be implemented that protects the **rights of the data subjects** (rights to information, access to and rectification or erasure of personal data, the right to data portability, the right to object, restriction of processing). This could be realised by providing an online form or email address to contact your company.

— Finally, the principle of **privacy by design** is considered fulfilled when, e.g., the data subject's consent is obtained prior to the data processing.

I have received business cards at an event. Is it permissible to add the data to my client database?

In principle, yes. In addition to a valid consent (and other legal prerequisites to be met), you have to clearly define the purpose of the data processing operation.

6 When is big data too big?

Big data applications have gained much ground with the digitalisation and the industry 4.0. Yet the GDPR clearly defines the extent to which automated data processing with regard to e.g., work performance or GPS location is permissible.

In the ongoing discussion about digitalisation and industry 4.0, "big data" is frequently mentioned. Big-data-based applications are able to collect, save and process vast and extensive databases. Companies can, for instance, increase the efficiency of their business processes or communication with customers based on the evaluation of such data.

Such datasets can also be used for what is referred to as automated decision-making, which enables companies to take certain decisions with regard to data subjects. Profiling, which is used to assess personal aspects of a natural person, is also a type of automated decision-making. By making us of profiling measures, features such as individual preferences, interests or location data are being analyzed and the results are consulted when making a decision, e.g. on a pay raise.

In the context of big data and profiling, you should keep in mind that they are also subject to the stipulations of the GDPR (e.g. data minimisation, purpose limitation and the general prohibition to process data unless a permission has been explicitly given). Moreover, special rules apply in the case of automated decision-making: they hold that the data subject (e.g. the employee) has the right not to be subject to a fully automated decision. This applies, if the decision becomes legally effective or has detrimental effects for the individual concerned.

An online recruiting process without any human intervention is an example for such a case. It follows that human intervention is a necessity in almost all situations. Exceptions to the requirement of human intervention apply when automated decision-making is necessary to enter into a contract or fulfil its terms or when the data subject has given his or her consent.

Implementing a pseudonymisation process might be a solution

In practical terms, this means that a company should give due consideration to the question whether or not to use personal data for big data analyses, particularly for profiling, to start with. Yet, many companies only notice that they are using data for such purposes when they are already processing them to this end. In such a case, the utilisation of an adequate pseudonymisation process might be a solution.

Who could bring legal action against me if I take data protection lightly?

Disappointed employees, unsatisfied (potential) customers and also competitors.

7 Be aware of the fines

Violations of the GDPR can be punished with fines that really hurt.

The GDPR will enter into force very soon. Breaches of its stipulations will then be fined: in an extreme case, a company might have to pay a penalty of up to EUR 20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever one is higher. Such fines could also be imposed on your company in the event of a serious breach. It is thus essential to take the necessary steps to implement a sound compliance system as soon as possible.

Why fines?

The sanctions stipulated in the GDPR are intended to deter companies from breaching data privacy regulations and to heighten the awareness that such infringements simultaneously violate the European fundamental rights. For this reason, the European legislator sought to impose fines that are effective, proportionate and dissuasive.

Are the authorities likely to impose the maximum sentence?

It is very difficult to answer this question, especially since most of the national Data Protection Authorities have not yet commented on the parameters governing the amount of the fine. Yet the GDPR has defined a number of criteria (which are, however, not final!) that Data Protection Authorities can consult when deciding on the amount of the fine.

What are those criteria?

They include the nature, gravity and duration and the intentional or negligent character of the infringement. Data Protection Authorities can also consider any relevant previous infringements and the manner in which the infringement became known to them (think of a voluntary disclosure) as aggravating or mitigating factors. The financial standing of the company could be a further significant criterion for setting the fine.

What are other potential penalties?

The national Data Protection Authority can make use of the powers stipulated in the GDPR and issue an order to terminate the infringement. To this end, it can, e.g., issue a warning or order the company to adapt its data processing operations to comply with the GDPR. The national Data Protection Authority can also prohibit any further data processing.

Are these rules final?

No, they are not, because the GDPR affords the possibility to national legislators to introduce further penalties.

How are breaches of compliance with regard to data privacy revealed?

On 25 May 2018, the function of the national Data Protection Authorities may significantly shift. It is expected that the Authorities will proactively carry out inspections. A dissatisfied employee complaining to the national Data Protection Authority can also kick off an investigation. The same applies to (potential) customers. With increasing size and popularity, companies can also be targeted by the press: investigative journalists might probe data protection practices to find a story.

What can you do?

- **Do not underestimate the importance of data protection to your company**: creating awareness for this topic early on is an important basis upon which to implement a compliance system.
- **Do not overestimate yourself**: data privacy is a complex matter and the points to be considered increase with the size of the company. For this reason, your company is well advised to seek expert advice on data protection and carry out compliance audits on a regular basis.

Your contact at CMS

Austria
Vienna
Johannes Juranek
T +43 1 40443 2450
E johannes.juranek@cms-rrh.com

Bosnia and Herzegovina
Sarajevo
Nedžida Salihović-Whalen
T +387 33 94 4600
E nedzida.salihovic-whalen@cms-rrh.com

Bulgaria
Sofia
Maria Harizanova
T +359 2 447 1350
E maria.harizanova@cmslegal.bg

Croatia
Zagreb
Marija Zrno
T +385 1 4825600
E marija.zrno@bmslegal.hr

Macedonia
Skopje
Marija Filipovska
T +381 11 3208900
E marija.filipovska@cms-rrh.com

Montenegro
Podgorica
Tamara Samardžija
T +382 20 416070
E tamara.samardzija@cms-rrh.com

Serbia
Belgrade
Ksenija Ivetić
T +381 11 3208900
E ksenija.ivetic@cms-rrh.com

Slovakia
Bratislava
Oliver Werner
T +421 2 3214 1414
E oliver.werner@cms-rrh.com

Slovenia
Ljubljana
Irena Šik Bukovnik
T +386 1 6205210
E irena.sik-bukovnik@cms-rrh.com

Ukraine
Kyiv
Maria Orlyk
T +380 44 5001718
E maria.orlyk@cms-rrh.com

About CMS

Staff
> 8,000

Lawyers
> 4,800

Partners
> 1,100

49 NEW PARTNERS IN 2019, TAKING THE TOTAL TO OVER 1,100

Operating in
71 cities

Across
43 countries

EUR 1.426bn
turnover for 2019

19 PRACTICE AND SECTOR GROUPS WORKING ACROSS OFFICES

- **#1 CEE, DACH, Germany** *(Mergermarket)*
- **#1 Germany, UK** *(Thomson Reuters)*
- **Top rankings in 2019 M&A League Tables** *(by deal count)*
  #1 by Bloomberg in Europe, Germany and UK
  #1 by Mergermarket in CEE, DACH and Germany
  #1 by Thomson Reuters in Benelux and Germany
- **#1 Europe, Germany, UK** *(Bloomberg)*

CMS offices

The Americas

Bogotá
Lima
Mexico City
Rio de Janeiro
Santiago de Chile

Europe

Aberdeen
Amsterdam
Antwerp
Barcelona
Belgrade
Berlin
Bratislava
Bristol
Brussels
Bucharest
Budapest
Cologne
Duesseldorf
Edinburgh
Frankfurt
Funchal
Geneva
Glasgow
Hamburg
Istanbul
Kyiv
Leipzig
Lisbon
Ljubljana
London
Luxembourg
Lyon
Madrid
Manchester
Milan
Monaco
Moscow
Munich
Paris
Podgorica
Poznan
Prague
Reading
Rome
Sarajevo
Seville
Sheffield
Skopje
Sof a
Strasbourg
Stuttgart
Tirana
Utrecht
Vienna
Warsaw
Zagreb
Zurich

Algiers
Casablanca
Johannesburg
Luanda
Mombasa
Nairobi

Africa

Abu Dhabi
Beirut
Dubai
Muscat

Middle East

Beijing
Hong Kong
Shanghai
Singapore

Asia-Pacific

CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.
cms-lawnow.com

CMS locations:
Aberdeen, Abu Dhabi, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Bergen, Berlin, Bogotá, Bratislava, Brisbane, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Cúcuta, Dubai, Dublin, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Gothenburg, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Liverpool, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Maputo, Mexico City, Milan, Mombasa, Monaco, Munich, Muscat, Nairobi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Riyadh, Rome, Santiago de Chile, São Paulo, Sarajevo, Shanghai, Sheffield, Singapore, Skopje, Sofia, Stavanger, Stockholm, Strasbourg, Stuttgart, Tel Aviv, Tirana, Vienna, Warsaw, Zagreb and Zurich.

Further information can be found at **cms.law**