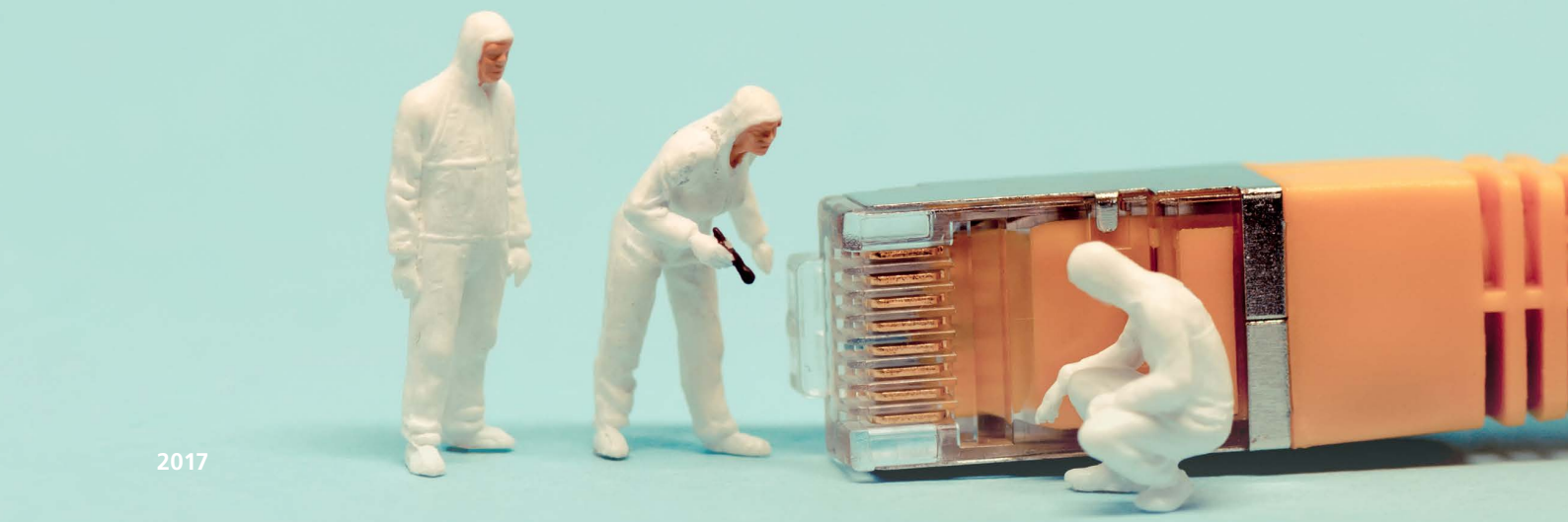
Your World First

C/M/S/
Law.Tax

Are you ready for the GDPR?: A conference report



2017

Overview

Emma Burnett
Partner, Head of Data Protection, CMS London

> The fines that organisations face in the risk of a breach of the new regulation is far more considerable than before and could be as much as €20,000,000 or 4 per cent of annual worldwide turnover.

There is a little over a year before the General Data Protection Regulation (GDPR) applies and the changes it will bring to the world of business are immense.

Many organisations could have to implement extensive changes to their internal operations and systems and, in some cases, even transform their business models before May 2018. The fines that organisations face in the risk of a breach of the new regulation is far more considerable than before and could be as much as €20,000,000 or 4 per cent of annual worldwide turnover. A shift in mindset could also be necessary in many companies as underpinning the new regulation is an 'accountability principle' which will require organisations to develop a holistic compliance culture. In short, 'taking a view' on data protection compliance is likely to become prohibitively expensive.

This new world could be particularly challenging in Britain where until now the implementation of the Data Protection Act 1998 has sometimes fallen short of both the requirements and the examples set by other Member States, such as Germany and France. The European Commission previously pursued infringement proceedings against the UK government for improperly implementing EU rules on ePrivacy and data protection. While this case was closed in 2012 in recognition of UK national law being updated to comply, the GDPR will be stricter. The GDPR could be just as demanding for example to American businesses that have not yet woken up to the reality that any company offering goods or services to data subjects in the European Union will have to comply with the new regulation or face substantial fines.

The European Article 29 Working Party and various Supervisory Authorities are in the process of issuing guidelines on the new regulation and it is essential for businesses and their advisers to keep abreast of these. Not least because under the GDPR the role and remit of Supervisory Authorities across the Member States is changing in some areas and there are a host of new requirements to adopt, from the appointment of Data Protection Officers to a new system of mandatory notification for data breaches.

Although there will clearly be challenges there will also be opportunities to develop innovative solutions and frameworks to help businesses, adapt to the GDPR. This conference report will hopefully begin the process of helping businesses prepare a GDPR implementation programme.

The accountability principle

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University

> This is not some theoretical concept or lofty aspiration, but a principle that will have a direct impact on how businesses operate.

The General Data Protection Regulation (GDPR) will apply from 25 May 2018 and will, subject to local derogations, harmonise much of the law relating to data protection across the EU. Crucially, it will require much closer co-operation between the different data protection authorities, or 'Supervisory Authorities', as they will be known.

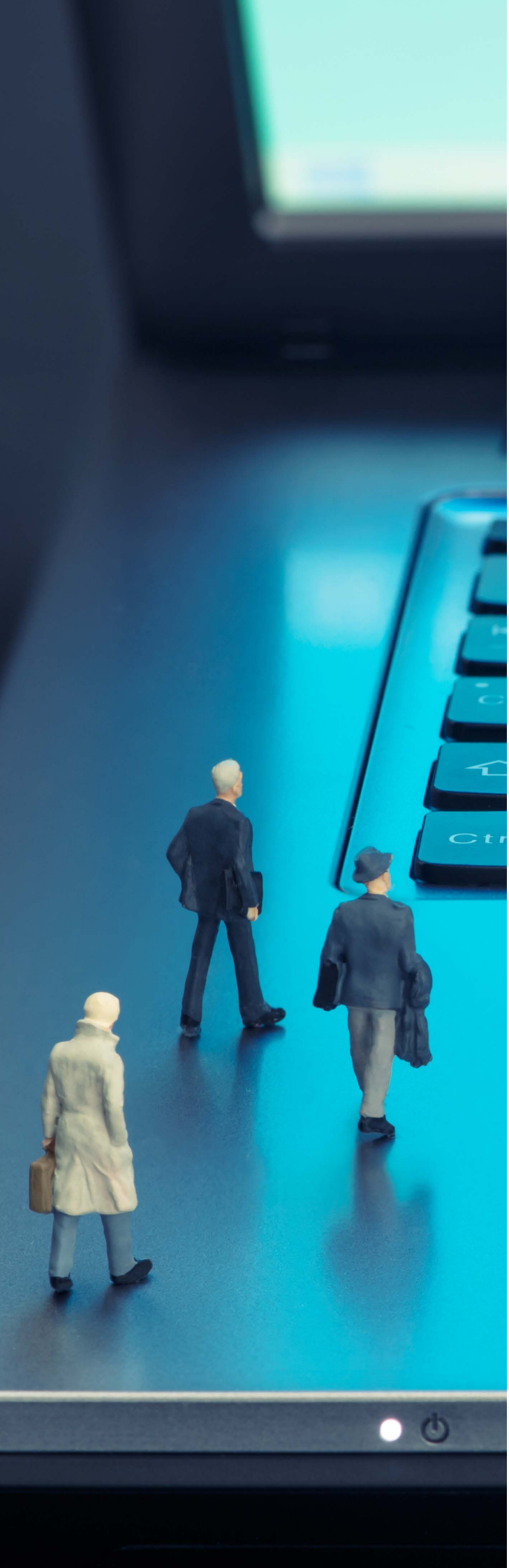
At the centre of this new regulation is the principle of 'accountability'. This is not some theoretical concept or lofty aspiration, but a principle that will have a direct impact on how businesses operate. In Britain, where the implementation of the Data Protection Act 1998 by organisations has sometimes been rather lax, understanding the importance of the accountability principle will be vital for businesses.

The accountability principle states that not only does a controller or processor of personal data have to comply with the principles of data protection, such as lawfulness, fairness and transparency amongst others, they must also be able to demonstrate such compliance.

In addition to giving effect to the accountability principle, the risks involved in processing operations should be assessed. Particularly risky processing operations, such as processing biometric data on a large scale, will require a formal data protection impact assessment. When risks are identified, appropriate mitigating measures should be put in place. A notification to the relevant Supervisory Authority will be necessary where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. Organisations should also be ready to respond to queries about risk assessments and any subsequent decisions taken.

Record keeping will be vital to demonstrate compliance and should involve keeping an inventory of processing operations. A simple description of databases is unlikely to suffice – an inventory should clearly distinguish between the different processing operations that take place in an organisation.

The GDPR also introduces the concepts of 'privacy-by-design' and 'privacy-by-default'. These must be embedded in the design of data processing operations.



The complex issue of determining who is a processor, a controller, or joint controller – an issue that has bedevilled data protection for a long time – has not been resolved yet. Under the GDPR, where there are joint controllers, they should have an arrangement that duly reflects their different roles and relationships vis-à-vis data subjects.

Controllers must keep a record of personal data breaches.

What is clear is that organisations will likely have to put in place comprehensive and proportionate governance measures to minimise the risk of breaches and uphold the protection of personal data.

For example, if a company is processing personal data on the basis of consent from an individual then it must show, amongst others, that adequate and specific information was provided to that person. If a company is asking to use data beyond what a reasonable person might expect then it could be necessary to draw particular attention to that request, explaining why it is required.

What does the GDPR mean for contracts?

Ian Stevens
Partner, CMS London

Tom De Cordier
Partner, CMS Brussels

Sam de Silva
Partner, Nabarro London

> Irrespective of the route taken, the process towards achieving compliance should have started already.

Unlike the position for data protection clauses under the Data Protection Act 1998, where there are generally accepted market norms for the contents and liability positions in relation to data protection, no such market for 'standard' or 'accepted' positions exist in relation to the GDPR. There are few published examples of clauses as yet, and many companies and their suppliers are still in the process of establishing their own compliance and risk positions. Suppliers in particular regularly simply resist inclusion of GDPR terms in contract negotiations stating: 'We are not ready yet – lets agree to agree something nearer the time'.

Where clauses can be agreed there is typically a two tiered approach – DPA clauses apply today, with an automatic rollover to GDPR-compliant clauses in May next year. Some organisations with more complex service arrangements are agreeing to collaborate with their suppliers to undertake due diligence, and devise and implement a transformation plan in an attempt to achieve compliance together.

Irrespective of the route taken, the process towards achieving compliance should have started already. Some companies have been slow to realise that areas of the new regulation, such as accountability, data privacy by design, data portability and erasure requirements, could require technological and business process changes both in their own business as well as in their suppliers' businesses.

Contract negotiations already under way or concluded have already revealed some contentious negotiating flare points.

Controllers requesting prior notification and specific approval if a processor wants to sub-contract processing operations can prove contentious where it creates an operational nightmare for suppliers which have dozens of sub-processors. Notification could involve stating why a subcontractor has been hired, where they are located and what data processing security measures are in place. Controllers do need to ensure compliance but suppliers may also feel aggrieved at perceived interference in their own businesses which could potentially put innovation at risk. The key consideration here will be how much control is ceded by both parties, the degree of future discretion that can be granted, and whether or not certain sub-processors and activities can be preapproved.

Audit rights, which are required under the new legislation, could become another key battleground. Controllers (particularly those operating in regulated sectors) will likely seek wide audit rights from their processors, and any sub-processors. They could seek to pass on audit costs to their suppliers and could insist on remediation plans in the event of a breach of data protection regulations. For their part, suppliers could object to 'invasive' audits deemed to have too wide a scope and which could jeopardize the confidentiality and security of their own data processes and technical and organisational measures. They may well argue that allowing every Tom, Dick or Harry into system infrastructure will only make it less secure against future hacking attacks. A compromise may be to engage trusted third party auditors to undertake regular comprehensive audits that can be relied on by both controllers and processors.

Determining liability in the event of breaches will likely also be a thorny negotiating point. Potential fines for breaches will be significant and most parties will balk at assuming unlimited liability. It may be necessary to cap liabilities and balance the risk between controllers and processors depending on where the fault for a breach lies. This is an area of particular importance as under the new regulation, Supervisory Authorities can now take enforcement action against both controllers and processors, whereas before they could only take action against the controller.

Contract negotiations are going to be tough and, while further guidance on the regulation is expected, starting early to avoid the anticipated future negotiation resource bottlenecks is advisable.

Issues and impact of the GDPR for employers

Graham Paul
Partner, CMS London

> There is a populist view that data protection is 'too difficult' and stops businesses from innovating and implementing new processes. This is a mindset that must change.

Many British companies have been paying lip service to the Data Protection Act 1998 for years, particularly when it comes to how they process employee data. Rightly or wrongly, they have often taken the view that the commercial, reputational and legal risk from a data protection breach is greater if it relates to third parties as opposed to their own employees. This is all about to change once the GDPR applies. How companies deal with employee data is vital given the sheer volume of such data most businesses hold, the sensitivity of that information, both real and perceived, and the speed at which data processing takes place on a day-to-day basis.

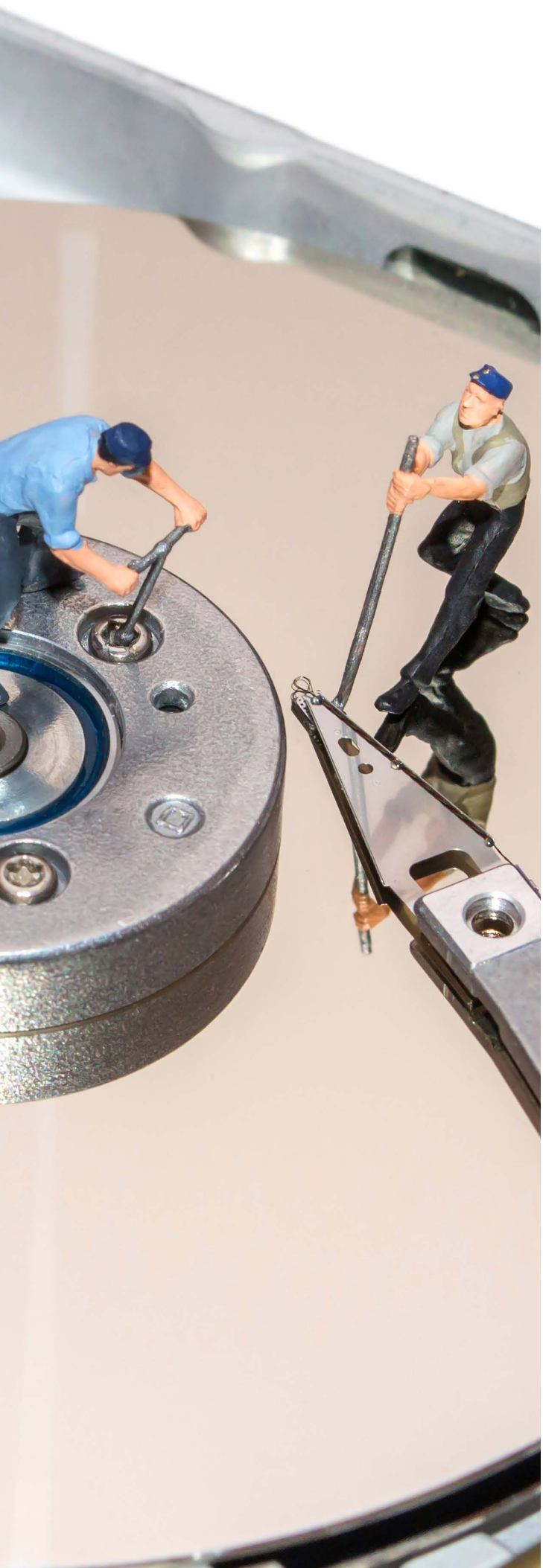
There are a number of tasks that should be undertaken now to help companies prepare for May 2018. The starting point is that human resources (HR) departments must be engaged and represented in any wider business GDPR task force or working party. Businesses should be selecting GDPR 'champions' in HR who can prioritise understanding the regulation and act as the company's ears on the ground once the regulation applies. There needs to be proper and continuous training, whether internal or external, of these champions.

There is a populist view that data protection is 'too difficult' and stops businesses from innovating and implementing new processes. This is a mindset that must change. Businesses need to work on getting HR teams familiar with the basics that exist now, in order that they have the building blocks to step up to the new regulation. HR champions do not need to become data protection experts but they must become proper gatekeepers for a business.

Businesses should also be carrying out a high-level audit of what employee data processes are currently taking place each day: from the gathering of data on recruitment and joining, through day-to-day processing to significant third party data transfers and relationships with third party vendors. This audit can be a written log of all processing activities that take place.

The next stage of the preparation process involves analysing what employee data is being held and deciding if it is all necessary. For example, it is unlikely to be necessary to store all of the data currently held on former employees or unsuccessful job applicants.

Companies must obviously also then consider what Article 6 and where relevant Article 9 conditions (the special categories of personal data) they will rely on when carrying out employee data processing. Conditions could include a company's processing that may be necessary for the purpose of legitimate interests as well as processing that may be necessary for the purposes of carrying



out the obligations and exercising specific rights of the controller or of the data subject in the field of employment law. It is essential to consider under what lawful basis employee data processing is taking place, as this will influence what documentation businesses must prepare.

While the popularity of Data Subject Access Request (DSAR) has arguably died down under the existing regulation, there could be a new flurry next year given that these are free of charge, except if manifestly unfounded or excessive.

Employee data protection is going to be a material issue for businesses going forward and compliance must be dialled up a good few notches. Having policies and procedures in place to help HR teams make the correct decisions when processing employee and third party data is essential. They can help derisk the system and, in the inevitable event of a breach, a regulator will be significantly more sympathetic if it is obvious that it was a human error rather than a systemic fault.

Updates from recent guidelines

Loretta Pugh
Senior Assoicate, CMS London

Christian Runte
Partner, CMS Munich

> The role of the Data Protection Officer (DPO) was only optional under the Directive but under the GDPR it will become mandatory in certain circumstances, for example for public bodies, and advisable for most large organisations.

In December 2016, the Article 29 Working Party (WP29) issued guidelines and FAQs on the Lead Supervisory Authority, Data Portability and Data Protection Officers. The WP29 welcomed comments on these guidelines until the end of January 2017.

Lead Supervisory Authority

Each jurisdiction in the EU has at least one Supervisory Authority, which in the UK is the ICO. Under the GDPR there is the concept of the 'Lead Supervisory Authority'. This is important in the context of cross border processing where a controller or processor has establishments or activities in more than one Member State. In such circumstances, the Lead Supervisory Authority has primary responsibility, for example in co-ordinating investigations, in registering a Data Protection Officer, notifying of 'risky' processing and the notification of security breaches. As a result it is important to correctly identify which Supervisory Authority will be the Lead Supervisory Authority in the given circumstances.

Identifying the Lead Supervisory Authority is not always straightforward. The GDPR states that the Lead Supervisory Authority is the Supervisory Authority of the 'main establishment' or the single establishment of the controller or processor.

'Main establishment' is a defined term in the GDPR. That definition is convoluted, but essentially, for controllers the main establishment is the establishment in the EU where decisions on the purposes and means of the processing of personal data are taken. For processors the main establishment is essentially the place of the central administration in the EU, or if that does not exist, then the establishment in the EU where the main processing activities take place.

Controllers may have to deal with more than one Lead Supervisory Authority depending on their structure and processing activities.

Although a controller may have establishments within the EU, if the decisions in relation to the purposes and means of processing activities are taken outside the EU, then there will be no Lead Supervisory Authority.

Data Portability

Data portability is a data subject right that gives a data subject the right to receive certain personal data and have certain personal data transferred to another data controller, where technically feasible, in a 'structured, commonly used and machine readable format' and where the processing is based on consent or on a contract and is carried out by automated means.

The GDPR states that personal data falling within the scope of the right must concern the data subject and must be that which has been provided to the controller by the data subject. However, the guidelines state that these elements should not be construed too restrictively. The data transferred can contain the personal data of others, provided it is not subsequently processed for any purpose that would adversely affect their rights or freedoms. In addition, personal data provided by the data subject is to be construed as not just that which is actively and knowingly provided to the controller by the data subject, but also 'observed data', which is that generated by the data subject's use of the relevant service or device, for example, a search history generated from an individual using a web browser.

So called 'inferred' or 'derived' data, being that generated by the controller from the analysis of the data provided by the data subject, such as a credit score, does not need to be transferred.

Controllers will need to consider how they envisage data subjects will request their data. It could, for example, involve the completion of a request form on a website or some form of self-service model whereby the data subject selects the data to be transferred and initiates the transfer resulting in a direct download of the data without any manual intervention by the controller.

As well as being 'structured, commonly used and machine readable' the format of the personal data transferred should foster the re-usability of the data. Controllers should consider offering various format options for data transfers.

Meta data should be transferred if useful to make sense or use of the data once transferred, however no additional meta data should be created on the basis that it may be useful to answer a data portability request.

Before any transfer takes place, a controller must verify the identity of the person making the request. In addition, the controller will be responsible for taking all security measures needed to ensure that personal data is securely transmitted, for example by the use of encryption.

IT system changes are likely to be required to meet the data portability requirements. Lead times for any changes to be implemented and tested could be significant, particularly where IT services are outsourced. Given these potential lead times, data portability may well be an area of GDPR implementation that organisation should be prioritising.

Data Protection Officers

The role of the Data Protection Officer (DPO) was only optional under the Directive but under the GDPR it will become mandatory in certain circumstances, for example for public bodies, and advisable for most large organisations.

The guidelines state it will be necessary to appoint a DPO when the core activities of a controller or processor consist of processing activities which require regular and systematic monitoring of data subjects on a large scale, or where the core activities of the controller or processor consist of processing on a large-scale of special categories of data or personal data relating to criminal convictions and offences.

A decision on whether to appoint a DPO rests solely with the controller or processor, which will require a level of interpretation of the guidelines. A hospital, for example, has a core activity of treating patients but also has to processes large quantities of personal data such as patients' health records. As a result the hospital would need a DPO. However, the processing of personal data by an individual doctor or lawyer falls outside the scope of requiring a DPO. Organisations should document how they arrived at the decision as to whether to appoint a DPO as the decision may be questioned at a later date.

A DPO must have a certain level of skill, such as a law degree, and they must always be independent and easily accessible to senior management, data subjects and Supervisory Authorities. DPO's will need to speak the language used by the relevant Supervisory Authority. The contact details of a DPO, for example an email address and phone number, must be readily available.

Organisations that appoint a DPO must ensure that their DPO is properly involved in a timely manner in all issues relating to the processing of personal data and given adequate resources and training. Although the opinion of the DPO is only advisory it should be given due consideration. If the advice of a DPO is not followed then the organisation must be prepared to explain why.

If a DPO is appointed voluntarily by an organisation all the provisions in the GDPR relating to DPOs will apply.

International data flows

Geraldine Dersley
Lead Solicitor and Head of Legal Profession, Information Commissioner's Office

It is hoped that organisations will become more accountable and think more holistically about establishing proper systems and procedures for data transfers rather than just relying on a particular derogation.

The understanding and awareness of the current data protection regulations around international data flows are well known. Broadly speaking, transfers can only be made to third countries if: there is a finding that the country in question has ensured an adequate level of protection that has been approved by the European Commission; if the transfer takes place under a specified derogation; if the data controller provides adequate safeguards, such as Standard Contractual Clauses or Binding Corporate Rules which have been approved by the Commission.

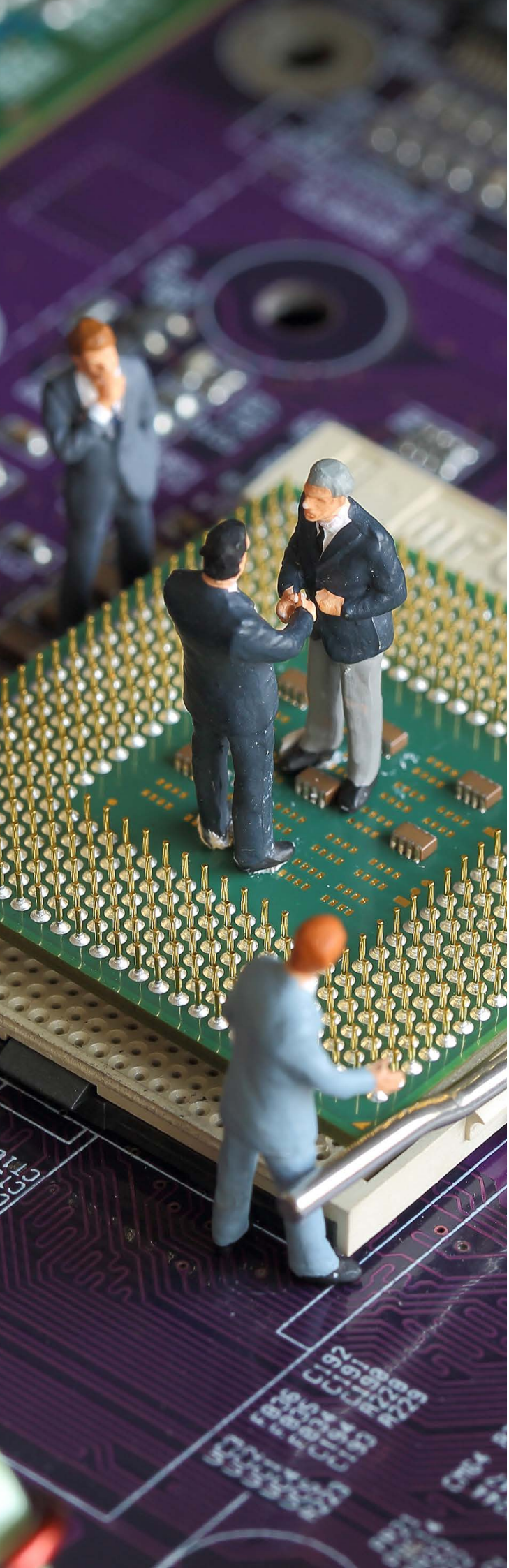
Under the GDPR the approach to international data transfers is broadly similar to the Data Protection Act 1998 although there are some key differences.

The main divergence is that a cumulative and systematic approach must now be taken to working through all the transfer mechanisms in order to assess if it is possible. It will no longer be possible to go straight to derogations, such as the use of consents which can sometimes cause more issues than they solve. The intention under the GDPR is authorisation by Supervisory Authorities of systems and arrangements for transfers rather than individual transfers. It is hoped that organisations will become more accountable and think more holistically about establishing proper systems and procedures for data transfers rather than just relying on a particular derogation.

Going forward, the starting point for any data transfer to a third country will remain the initial consideration of whether it is even necessary to send personal data. If it is deemed necessary then it must be considered whether that data can be anonymised.

Once a decision has been made to transfer data then the first mechanism to be considered is an adequacy ruling. Can the third country or specified sectors or an international organisation receiving the data ensure an adequate level of protection? Under the GDPR there appears to be a reduced role for Supervisory Authorities in making adequacy rulings which will be made by a committee of representatives of the Member States.

In the absence of an adequacy finding, transfers can be made where the controller or processor has provided for adequate safeguards including: binding corporate rules; approved standard data protection clauses adopted by the Commission or Supervisory Authorities and approved by the Commission; codes of conduct with binding and enforceable instruments and certification mechanisms, seals and marks with binding and enforceable commitments. The level of involvement of Supervisory Authorities will be different depending on the type of safeguard. For example,



Binding Corporate Rules will, for the first time, have a legislative basis and will have to be approved by a competent Supervisory Authority in accordance with the consistency mechanism. When it comes to standard contractual clauses, the GDPR has indicated these can be adopted by the Commission or by a Supervisory Authority and approved by the Commission.

For the first time safeguards such as a code of conducts along with certification mechanisms can provide a new basis for data transfers. Supervisory Authorities are to encourage drawing up of codes to be approved by the Supervisory Authorities. If data processing is taking place in more than one Member State then the code must be submitted under consistency mechanisms to the European Data Protection Board (EPDB) and to the Commission.

Certification, seals and marks could be approved by a Supervisory Authority or certification body. Key will be assessing what binding and enforceable commitments, or other legally binding instruments, will be needed to make data transfers under this new mechanism work.

International data transfers can also still be made under ad hoc arrangements. These can include contractual clauses between a controller or processor exporting the data and the recipient in the third country or international organisation, provisions inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights, and authorisation required by competent Supervisory Authority via the consistency mechanism.

In the absence of any of the above bases of transfer, data may only be transferred under a specific derogation, including fully inferred and explicit consent of the data subject, necessary for the performance of a contract or implementation of pre-contractual measures at the data subject's request, or necessary for the inclusion or performance of a contract in the interest of a data subject but between the controller and another person (although these do not apply to the activities of a public authority, exercising its public powers). Further derogations exist in respect of processing that is necessary for important public interest, establishment, exercise or defence of legal claims, vital interests of data subject or made from a request intended to provide information to the public.

Where no other safeguards or derogations apply, and the exporter is not a public authority, then a transfer can only take place if it is not repetitive, concerns only a limited number of subjects and is necessary for a compelling legitimate interest. Even then, it is necessary for the controller to have assessed all the risks, provided suitable safeguards and informed both the Supervisory Authorities and the data subject.

GDPR: the trade-offs

Shanker Singham
Director of Economic Policy and Prosperity Studies, The Legatum Institute

Victoria Hewson
Senior Associate, CMS London

> Britain could possibly struggle to maintain its status as a safe and adequate destination for data in the future given domestic legislation, such as the Investigatory Powers Act...

When discussing GDPR, the elephant in the room is Brexit. The new data protection regulation applies next May at which time Britain will have already triggered Article 50 and will be part way through a two year process of exiting the European Union.

Britain will not just be in negotiations with the European Union but it will also be immersed in trade discussions with the US and a host of other key trading partners, such as India and China. There could be group negotiations with allied countries, such as Australia, New Zealand and Singapore under way and unilateral considerations, such as potential tariff reductions, will also need to be taken into account. Any agreements that come out of these discussions must sit alongside the World Trade Organisation rectification process – which Britain has already begun.

It goes without saying there will be a host of competing objectives and finding ways to reconcile these different objectives in a way that is workable for business could be complex. The UK may have to make some choices and that could have implications for trading arrangements around the world.

The incoming GDPR will form a key consideration in many of these negotiations, particularly in discussions with the US where the issue of data flow is extremely important to American companies but can cause tension with the policy objective of protecting personal data. In the past such concerns have been resolved by Safe Harbour and more recently via the Privacy Shield and that could continue to be a mechanism that is used.

In Europe, Britain could possibly struggle to maintain its status as a safe and adequate destination for data in the future given domestic legislation, such as the Investigatory Powers Act which makes provisions for the interception, acquisition and retention of communications data. As part of the Union, such powers have not been seen as an obstacle to data protection as there was a full national security exemption as part of the EU Treaty but Britain may no longer be able to rely on that going forward.

A decision point is also likely to come where Britain could start to ask if the GDPR is the best possible data protection solution for the UK and its economy. There are potential risks if Britain goes down this path, however, as the more it diverges from the GDPR framework it could further jeopardize the safe country status. But it is also important to consider that nothing remains static and if the EU were to further change the data protection regime in the future then Britain would only be an observer and would have no input as

it did in the formulation of the GDPR. Is that a sustainable situation in the long term? It may well be that a decision will be taken that the benefits and opportunities from streamlining or improving Britain's domestic data protection regime are greater than the potential disadvantages of diverging from the EU.

Britain should be keeping a close eye on how the Swiss authorities are currently dealing with their own GDPR compliance issues. There is currently draft legislation under way which seeks to update the country's Federal Act on Data Protection to bring it in line with the GDPR. The preliminary draft follows the principles and the approach of the GDPR to the letter in some cases, but in general terms it is a lighter touch approach–fines for breach are capped at CHF 500,000 Swiss Francs as opposed to the much higher fines under the GDPR. The outcome of the revised Swiss Federal Act on Data Protection could be a test of what could lie in store for Britain.

Cyber security and breaches

Christopher Burgess
UK Cyber Leader, AIG

Stephen Tester
Partner, CMS London

Andrew Harbison
Director, Grant Thornton

Tom Scourfield
Partner, CMS London

> A sobering reality is that no matter how sophisticated a cyber-security system is the weakest link remains the 'wetware', or humans using the systems.

Andrew Harbison, a white hat hacker and instant response specialist at Grant Thornton, said there is every reason for businesses worldwide to feel threatened by potential cyber breaches because it is inevitable they will happen. Since 2005 the statistics show there has been an exponential increase in hacking, malware and social engineering breaches. Nothing is out of bounds - where once the bad guys went after web servers and file servers they now attack peoples' mobile phones. The rates of detection of hacks and fraud are also declining.

A sobering reality is that no matter how sophisticated a cyber-security system is the weakest link remains the 'wetware', or humans using the systems. Research shows that the amount of time a phishing email stays on a network before being clicked is less than an hour and probably less than 15 minutes. This means some hacks may be simply unstoppable and that is why incident response planning is a crucial matter.

Companies should always have an incident response ready to avoid panic in the event of a cyber-breach. The first few minutes of an incident are vital and the success of the response will depend enormously on the level of planning already carried out.

Well-formed incident response plans should include details of where the server logs and work service logs are located and who should be consulted in the event of a breach from internal staff to external advisers. Many companies react before understanding the full nature of the problem which can be counter-productive. It is best to not panic and assess the best course of action before heading off half-cocked.

Tom Scourfield, one of the founding partners in the CMS Cyber network response team, – explained that one of the key pillars of any incident response is bringing in forensic and legal advisers and the sooner that is done the better. The biggest legal risk faced by companies is typically the loss of client, customer or employee personal data – a breach that, post GDPR, must in many instances be reported to the regulator within 72 hours of the attack. While forensic experts can help determine the source of the breach, a good lawyer can help chart an effective strategy to manage the incident and protect legal privilege in the event of future third party claims.

Notifications to third parties, such as service providers or to the affected subjects, should always be handled extremely carefully. Any notification should not only inform a subject of the breach but should provide helpful details on what is being done to rectify the situation and what they can do constructively – changing passwords, for example. There should also be a consistent message throughout which can be difficult in fast-moving situations and 'front end staff', such as call centre employees that are interacting with customers, should be kept informed. If helpful, a company can pre-prepare templates and guidance for staff to help manage notifications.

Under the GDPR there will be a legal obligation to notify in many circumstances and what the Supervisory Authorities will be looking for in a response is sensible decision making based on an informed understanding of risk and resultant action and planning. It is advisable to write a report at the end of the 72 hour initial period to document decisions taken which can be helpful in demonstrating that a response was proportionate and responsible, particularly as the factual background may change with greater understanding of the incident, so the context of that initial decision making can be lost if not recorded.

Many companies may choose to take out a cyber-insurance cover which may not address all eventualities but can often work well in conjunction with other policies, such as professional indemnity policies. Christopher Burgess from AIG said policies will need to be tailored to the business model as companies will have different exposures. Some policies, such as those provided by AIG, include event management or 'first response' coverage which can help a business manage those crucial initial hours. No matter how small or large a company or how sophisticated its 'cyber posture' it can be useful to have a team of crisis management experts to work alongside shoulder-to-shoulder to figure out how to handle a breach.

Contacts

The CMS contacts listed below were speakers at the conference. If you would like further detail on the outcomes of their panels, please get in touch.

Alternatively, get in touch with your usual CMS contact who will be more than happy to answer or redirect any specific questions you have.

Emma Burnett
Partner, Head of UK Data Protection
CMS London - TMIC
T +44 20 7367 3565
E emma.burnett@cms-cmck.com

Christian Runte
Partner, Global Co-Head of Data Protection
CMS Munich - TMIC
T +44 20 7367 3565
E christian.runte@cms-hs.com

Ian Stevens
Partner,
CMS London - TMIC
T +44 20 7367 2597
E ian.stevens@cms-cmck.com

Graham Paul
Partner,
CMS London - Employment
T +44 20 7367 2458
E graham.paul@cms-cmck.com

Tom Scourfield
Partner,
CMS London - TMIC
T +44 20 7367 270
E tom.scourfield@cms-cmck.com

Stephen Tester
Partner,
CMS London - EIRG
T +44 20 7367 2894
E stephen.tester@cms-cmck.com

Tom De Cordier
Partner,
CMS Brussels - TMIC
T +32 2 743 69 13
E tom.decordier@cms-db.com

Lorretta Pugh
Senior Associate,
CMS London - TMIC
T +44 20 7367 2730
E lorretta.pugh@cms-cmck.com

Victoria Hewson
Senior Associate,
CMS London - TMIC
T +44 20 7367 3602
E victoria.hewson@cms-cmck.com

Sam de Silva
Partner, Nabarro
Contact details to be confirmed 1 May 2017


Aberdeen
Glasgow
Edinburgh
Moscow
Hamburg
Amsterdam
Berlin
Warsaw
London
Utrecht
Duesseldorf
Leipzig
Bristol
Antwerp
Cologne
Kyiv
Brussels
Frankfurt
Prague
Luxembourg
Vienna
Paris
Stuttgart
Strasbourg
Munich
Bratislava
Zurich
Budapest
Geneva
Lyon
Ljubljana
Zagreb
Milan
Belgrade
Bucharest
Sarajevo
Sofia
Podgorica
Barcelona
Rome
Tirana
Istanbul
Madrid
Lisbon
Seville
Algiers
Tehran
Casablanca
Medellín
Bogotá
Mexico City
Dubai
Muscat
Lima
Beijing
Rio de Janeiro
Shanghai
Hong Kong
Santiago de Chile

CMS Cameron McKenna LLP
Cannon Place
78 Cannon Street
London EC4N 6AF

T +44 (0)20 7367 3000
F +44 (0)20 7367 2000

1703-0086-8