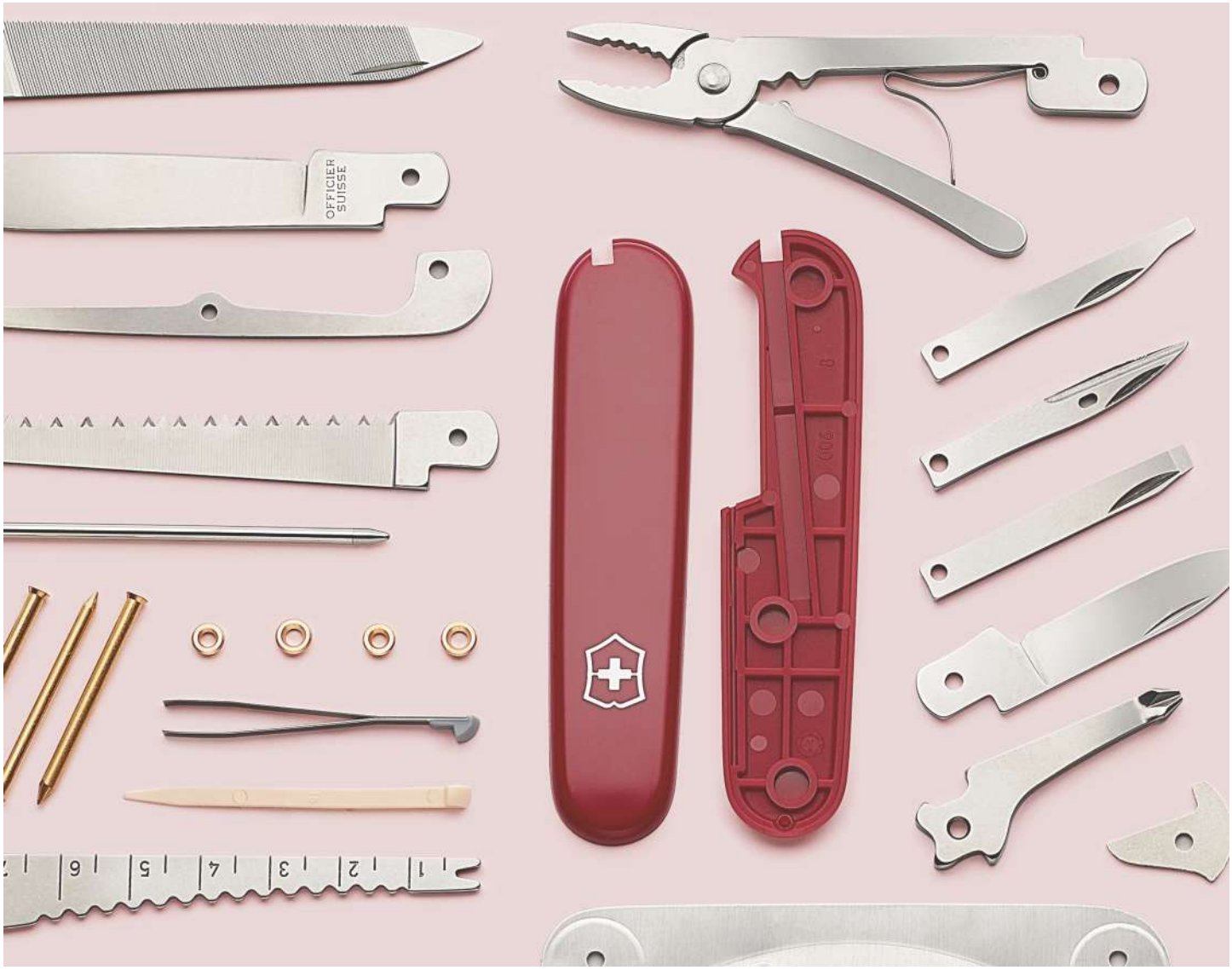
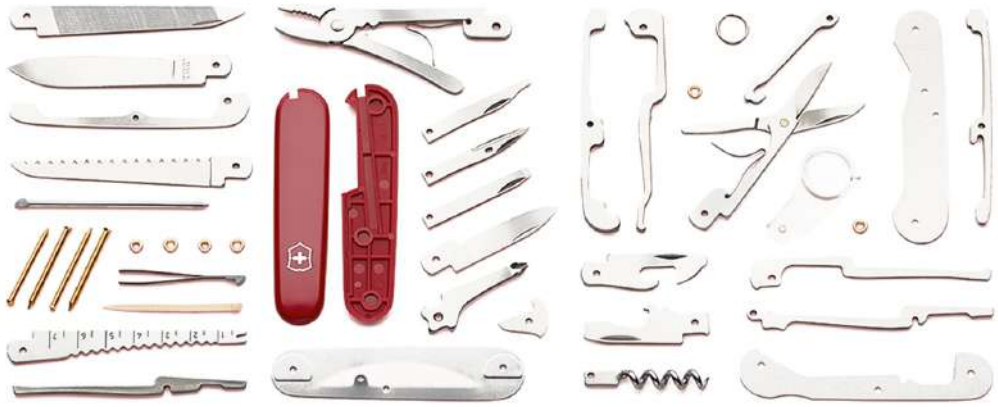
Burness Paull

Getting Ready for the General Data Protection Regulation



TECHNOLOGY

ON YOUR MARKS / GET SET



The data protection and privacy landscape is changing. The way we handle personal information will need reconsideration. And this will bring challenges for us all which will require new tools to overcome the changes.

The shift in law is primarily driven by the European Commission through the new General Data Protection Regulation.

Whilst the Regulation will fundamentally alter the existing data protection framework, a number of other pressures are impacting the way information is handled. The finding that the US Safe Harbour scheme is invalid (this was a mechanism to enable personal information to be transferred from Europe to the US) is likely to have further repercussions for the privacy landscape.

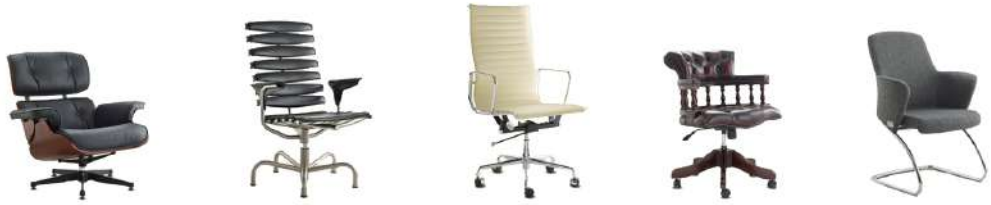
The Regulation will come into force on 25 May 2018. There's a lot to get to grips with. We know this. That's why this guide has been prepared to help you get started.

Our aim – to demystify the legal jargon and to tell you what you actually need to know.

This document provides an overview of the key challenges. We'd love to hear from you if you have specific questions.

Now, it's time to get ready...

CHANGES / CHALLENGES



Getting engagement from your colleagues, management or service providers can be hard. Engagement is so important because data protection filters through the whole of an organisation.

All EU organisations which process personal data need to comply with the new rules. The Regulation will also need to be complied with by non-EU organisations that (a) direct goods and services to EU individuals; or (b) monitor EU individuals.

Any use of personal information will need to be checked. This extends to online, automated and electronic use of personal data, which is why the data protection changes are relevant to the work you do.

What do you need to know?

- The new Regulation is intended to replace the existing European data protection law which includes the UK's Data Protection Act 1998 on 25 May 2018.

- Brexit considerations aside, it is intended that the Regulation will be "directly effective" in the UK. In other words, the UK government will have limited scope to apply a "British gloss" in their own legislation.

- The most notable change is increased fines for breaches of the regime. Fines of up to 4% of annual worldwide turnover or 20 million Euros (whichever is highest) are proposed. This will also lead to significant reputational damage.

What do you need to do?

- Get engagement at each part of the business early on. Management need to be aware of the monetary penalties for non-compliance.

- Audit what personal information you hold, why you hold it, what you do with it and on what terms you received or generated the information (e.g. directly from a customer, via an employment contract or from a third party supplier).

TIME TO TAKE NOTICE

The current law requires organisations to provide a "fair processing notice" to ensure that those affected by use of their personal information understand what their information is being used for. Notices can take different forms depending how you are receiving and handling data. Typically just now they are bundled into terms and conditions or privacy policies.

The new Regulation doesn't change this general position. Instead, in an agenda of "openness" and "transparency", the Regulation expects much more information to be supplied to individuals in an up front manner.

It's time to take more notice of what you are doing...

What do you need to know?

- Extensive information must be supplied by an organisation in a fair processing notice. (Please see Appendix 1 which shows the information to be included in the notice.)

- Notices need to be concise, transparent, intelligible and easily accessible, taking into account who is reading the notice.

- You need to think about when you give notice to individuals who are affected by use of their information. The Regulation expects notice to be given at the time information is collected from an individual. This may not be practical in all cases, for instance, if you have received data from a third party. In this case a notice would need to be given: (a) within one month of collection of the data; (b) at the time you first communicate with the individual concerned; or (c) before you disclose the information to a third party.

- The Regulation introduces a new principle of "accountability" where organisations need to be able to demonstrate how they comply with the regime. Notices will be part of this mix.

- Businesses will also need to keep a record of processing activities (akin to the notification required by the regulator).

What do you need to do?

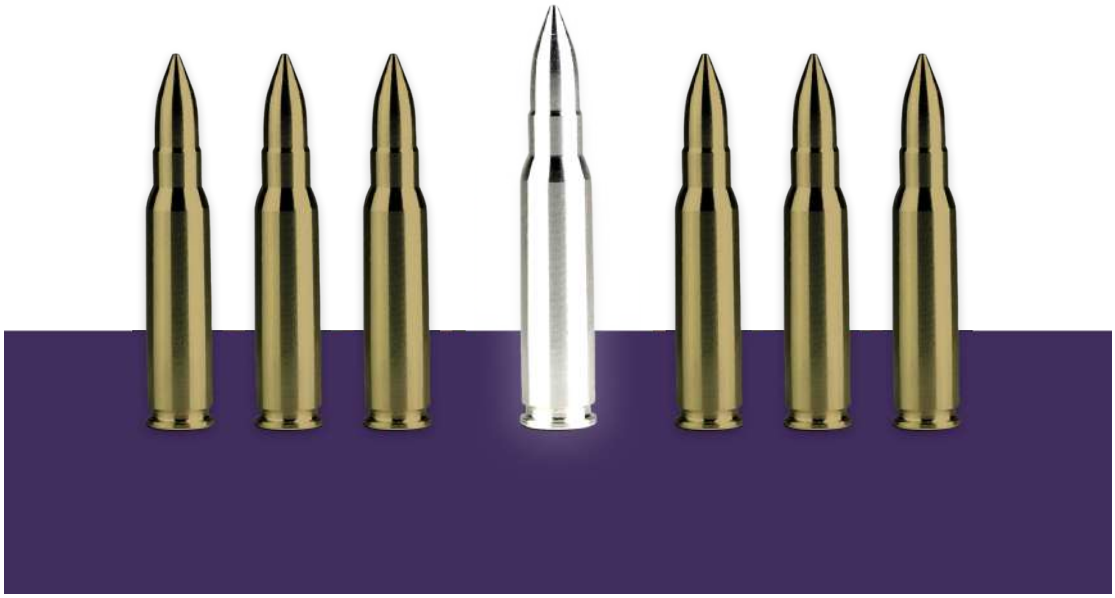
- Existing fair processing notices should be checked. This will require a legal review, but different parts of the business (including IT) should also be involved in this to ensure notices are clear and concise, and accurately reflect how data is used by the business.

- IT will likely be involved in considering new methods of how notices are made available to individuals. Hiding a privacy policy at the bottom of a website will no longer be sufficient – how can you make notices more visible?

- New technologies may need to be developed to help monitor and record when personal data is collected and what notice was given at the time. We expect audits of how data protection is collected and used will become more commonplace in order to help demonstrate "accountability" under the new regime.

- Guidance underlines that consent should be avoided as a processing ground in the context of employment.

CONSENT / THE SILVER BULLET?



The current regime overstates the use of "consent" to give a right to use personal data. It is often mistakenly seen as the "silver bullet" - giving an organisation all the rights they need to use data. That's true in many respects and consent is a requirement in the case of using data for electronic marketing.

However for uses other than electronic marketing, consent is just one way to process personal data. The existing regime gives a number of other options called "fair processing conditions" to enable an organisation to use personal data. The new Regulation continues to provide for this. These other options are worth considering because the Regulation is going to make it harder to use consent.

So before you pull the trigger...

What do you need to know?

- To rely on consent as a route to using personal information, you need to show that consent is "*freely given*", "*specific*", "*informed*" and "*unambiguous*" and delivered through a "*clear affirmative action which signifies agreement to personal data relating to them being processed*".

- Consent should be "*distinguishable*" – in other words, it should be separate from other matters. Consent hidden away in general terms and conditions will no longer be acceptable.

- New factors are introduced to ascertain whether further processing of existing data is legitimate.

What do you need to do?

- Review your legal basis for use of personal information. This may seem like a job for the legal team, but all aspects of the business will need to get involved to ensure that all bases are covered.

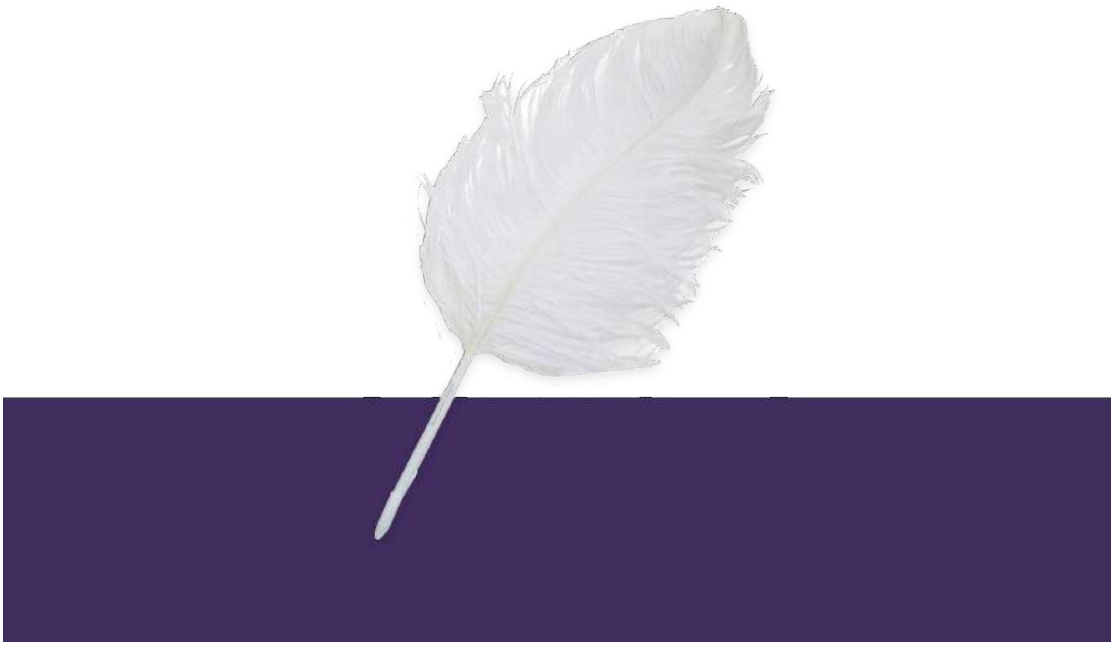
- If you have relied on consent for the collection and use of some personal data, the way consent was obtained will need to be considered. Did the individual undertake a "*clear affirmative action*" when giving consent?

- Consent may need to be re-affirmed in line with the new requirements. This may involve conducting a mass-communication exercise (particularly if customers are involved).

- The existing regime provides other grounds to process personal data which are listed in Appendix 2. These grounds might be more appropriate.

- Don't forget that sensitive personal data needs a further fair processing ground. See the next section.

TIME TO GET SENSITIVE



A key change which will be brought about by the Regulation is a reform of the concepts of "personal data" and "sensitive personal data".

Over recent years it has become increasingly difficult to pinpoint which category information may fall into. Is an anonymous spreadsheet of individual statistics personal data if another spreadsheet can be used to de-code it? Is information about online habits personal data? What about technical information collected from a smart meter or app? What about location data?

What do we need to get sensitive about here?

What do you need to know?

- The definition of "personal data" under the Regulation has been widened to specifically include location data, online identifiers or other factors specific to an individual.

- Sensitive personal data, or special categories of personal data, now includes genetic data and biometric data which is processed to uniquely identify an individual.

- Processing of sensitive personal data is prohibited unless at least one special processing ground applies. These special processing grounds are similar to the grounds for processing personal data, but with some key differences. Please see Appendix 2 for a list of the special processing grounds.

- The Regulation introduces a new concept of "pseudonymisation" - personal information which is processed in such a way that it no longer identifies individuals - provided additional information which can be applied to it to no longer make it anonymous remains separate. Use of pseudonymisation will help demonstrate compliance with the Regulation.

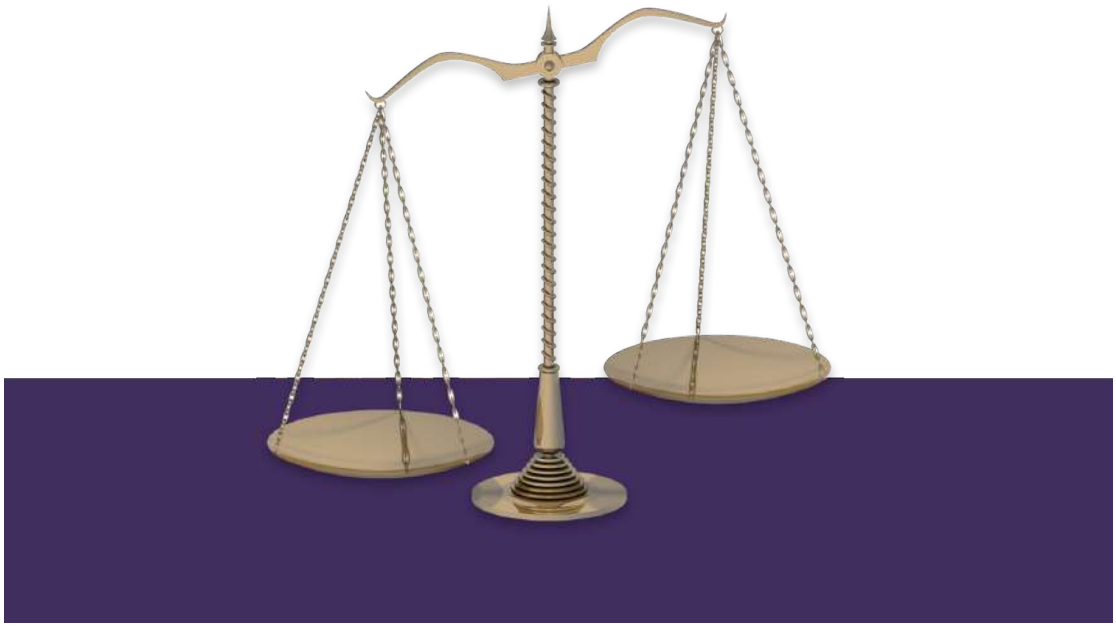
What do you need to do?

- Consider the information that you collect and process and whether or not this information could fall within the wider definitions of "personal data" and "sensitive personal data".

- If you rely on consent to process sensitive personal data, review your procedures to ensure the consent obtained meets the new standards.

- Given the inherent flaws in consent, it may be prudent to consider whether another special processing ground can be relied upon.

MORE RIGHTS / MORE OBLIGATIONS



The Regulation will introduce a number of new individual rights and some enhancements to existing rights.

For IT teams this poses a particular challenge, as electronic data will need to be stored and managed in such a way that it is easier to search, copy, update, transfer, extract, delete... the list goes on.

More rights leads to more obligations for organisations...

What do you need to know?

- Data Portability

The right to data portability is intended to make sure individuals have easy access to their personal data, so that they can move, copy or transfer personal data across different systems.

The use of the Midata system by the personal banking industry is an example of data portability. A version of this is likely to extend to utilities, as customers may expect access to their energy usage data in order to compare tariffs. This right only extends to data provided by an individual in certain specific cases.

- Strengthening Subject Access Rights

Subject access rights have been enhanced. In particular, subject access requests will need to be responded to within one month (rather than the existing 40 days), leaving less time for systems to be searched and relevant information to be collated.

- Right to be Forgotten

The right to be forgotten, synonymous with the well-known case against Google in 2014, is extended in the Regulation and will be exercisable by individuals against any organisation which controls their personal information. This only applies to data which an organisation cannot justifiably continue to process.

- Right to Object to Processing

Individuals can object to how you handle their information for a specific purpose. If an individual objects, you will have to stop the processing unless they can demonstrate that your interests override the individual's interests (a high bar!). In the case of an objection to processing for direct marketing, the right is absolute and the processing has to stop.

- Right to Restrict Processing

Individuals have the right to restrict processing, which means information can be stored but that any other use is temporarily blocked. This can be exercised in conjunction with existing rights – for example, if an individual objects to the use of their data, that data may be restricted while an organisation considers if they can justify processing the data. Restricted processing can also be exercised where an individual no longer wants an organisation to use their data, but does not want it to be destroyed (or "forgotten") in case they need it for a legal claim.

What do you need to do?

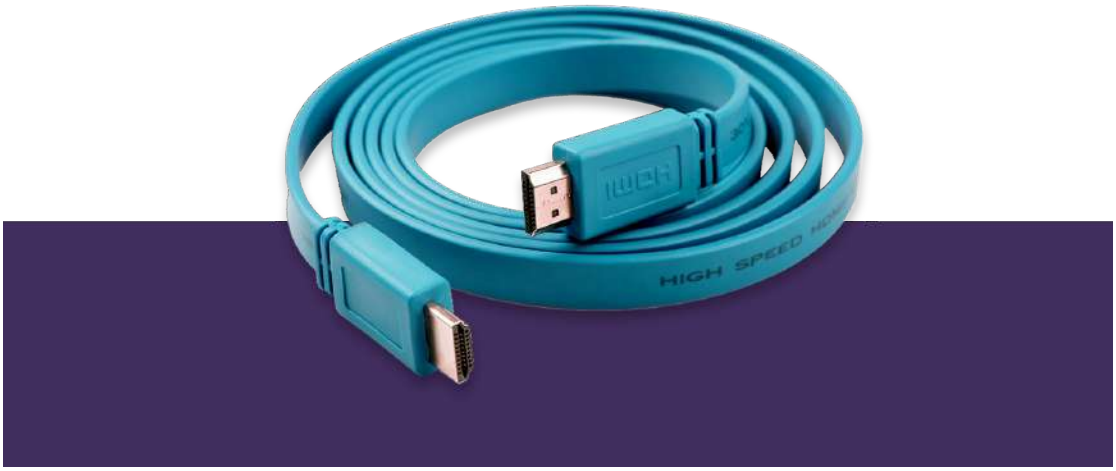
- Steps should be taken to ensure data processes and systems are set up in such a way as to take part in a Midata type system. If not, solutions may need to be considered relating to the storage, format and portability of customer personal data in particular.

- Think about your procedures for handling subject access requests. Are you currently able to deal with requests within a month? If not, consider how efficiency could be increased – do searching facilities need to be upgraded so that information can be collated quicker? Should data be stored in a more structured format

- Data retention policies can be useful to help demonstrate compliance – but can also reduce the amount of information which has to be considered when responding to requests.

- IT systems may need improved to comply with these rights – for example, can you completely erase personal information from your systems if an individual exercises their right to be forgotten? If an individual asks for their information to be restricted, can it be stored separately to ensure any other use is blocked?

PROCESSOR / CONTROLLER / DOES IT MATTER?



The Regulation is set to fundamentally change the existing legal relationship between data controllers and data processors.

At the moment, the responsibility for complying with data protection laws lies almost entirely with the data controller. Where a controller decides to outsource it's processing of data to another company (such as an IT service provider), they remain on the hook if, for example, the processor suffers a data security breach.

But not anymore...

What do you need to know?

- The Regulation introduces obligations which apply directly to data processors. Some of these are applicable only to processors, and others place obligations on controllers and processors alike.

- In particular, processors will have to ensure they have appropriate technical security measures in place, maintain records of processing activities and notify the controller if they suffer a data breach.

- Processors are also prohibited from sub-contracting out their processing without the consent of the controller. If the controller does consent, the processor will be fully liable for the data protection breaches of their sub-contractors.

- The processing of personal data by a processor will still need to be governed by a written contract. The Regulation expands upon the obligations which the processor is required to commit to under the contract regarding data protection. A list of the main points which will need to be addressed in contracts between controllers and processors going forward are set out in Appendix 3.

- Processors can be directly liable to individuals who suffer as a result of the processors' breach of the Regulation, and they can also be fined by regulators. The fines for processors will be set at a lower level – although this will still be the higher of €10 million and 2% annual worldwide turnover, so not insignificant.

- At the moment, it is unclear how fines may be apportioned between processors and controllers, however it is unlikely to be the case that controllers will be able to complete insulate themselves from liability with robust contractual protections, given that they are subject to a higher level of fine.

What do you need to do?

- Consider what contracts you have in place with suppliers that process personal data for you. This could include smaller contracts with app designers and marketing agencies, to larger-scale outsourcing or cloud service contracts.

- Consider revising tender processes when selecting data processors to ensure that they are able to meet all their obligations under the Regulation.

- Consider carrying out a data protection audit to gauge how much may need to be done to ensure compliance with the Regulation, including reviews of existing contract styles, policies and procedures.

DATA PROTECTION OFFICER / TO APPOINT OR NOT TO APPOINT?

Under the Regulation, there may be a need to appoint an over-arching Data Protection Officer (DPO), with ultimate responsibility and oversight over compliance.

The requirement to appoint a DPO has been watered down in the final text of the Regulation, leaving it in many places for local regulators to determine cases where a DPO is required. However, in light of increased obligations, it is likely a DPO will be needed by most organisations even if not prescribed by the Regulation.

What do you need to know?

- Organisations with core activities involving the regular monitoring of individuals on a large scale or the large scale processing of sensitive data will need to appoint a DPO. Public authorities will need a DPO.

- Member States can add their own requirements, so this is an area which will need review by the UK authorities.

- Responsibilities of DPOs will include monitoring their organisation's compliance with its data protection policies and data protection laws generally and co-operating with and serving as the organisation's contact for discussions with the ICO.

- A group of undertakings such as a corporate group may appoint a single DPO.

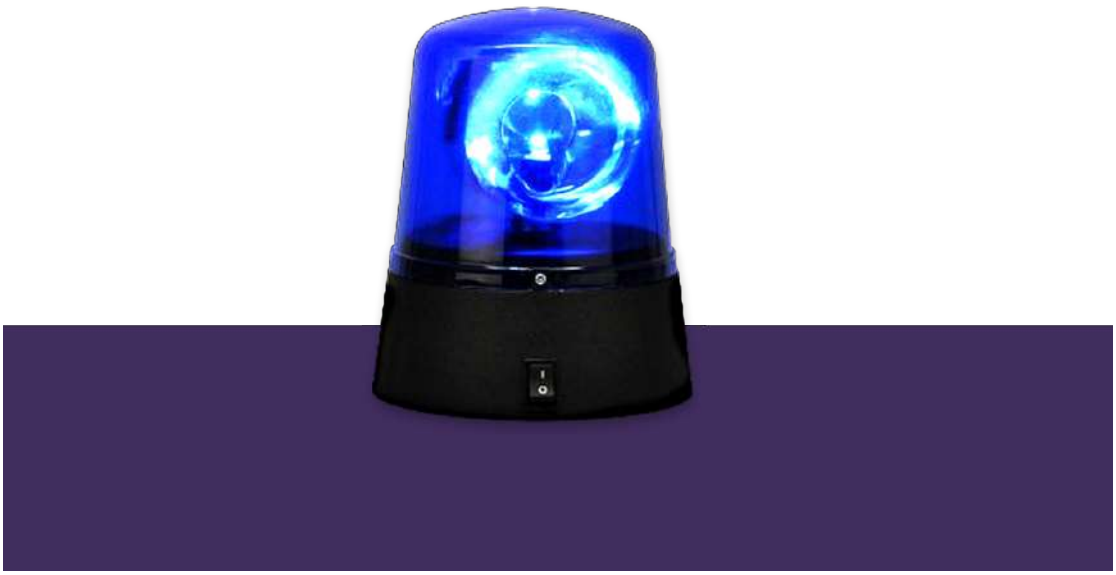
What do you need to do?

- Consider existing governance regimes for monitoring data protection compliance, to ascertain whether the responsibilities of a DPO are already being met.

- Is there an overarching individual who could be appointed the named DPO? Does this person have the necessary independence from the rest of your business in order to carry out the role with autonomy?

- Recent guidance has confirmed that if you do appoint a DPO even if not required to, the DPO will need to comply with the DPO rules set out in the Regulation.

SECURITY BREACH ALERT!



Perhaps the biggest data protection risk that most companies face is ensuring that information is kept secure. This is clearly easier said than done, with high profile stories of mass data breaches becoming everyday news (recently Yahoo! and Sage, and not forgetting Ashley Madison, TalkTalk and Morrisons).

The amount of reputational damage a data security breach can cause cannot be underplayed, and there is often a corresponding fall in share price as well. The Regulation is introducing a much higher level of regulatory fine for data security breaches.

The way data breaches are regulated is also changing under the Regulation.

What do you need to know?

- A data security breach will attract the highest level of fine under the Regulation – the higher of €20million or 4% annual worldwide turnover for controllers.

- The Regulation includes new obligations to report data security issues that affect personal data to the relevant national data protection authority. Breaches need to be reported within 72 hours. Corresponding with the regulator on data security breaches will be one of the responsibilities of the DPO.

What do you need to do?

- The first step will be to ensure that internal reporting procedures for data security breaches are up to scratch. In order to be able to report to a national authority, there needs to be robust processes internally to ensure the DPO is made aware of breaches.

- The impact of the higher level of fines may push data security matters up the priority list for management. Now may be a good time to consider how existing systems could up upgraded or bolstered with better technology to protect personal data.

ASSESSING YOUR IMPACT

Privacy impact assessments (PIAs) are a means of helping organisations identify and reduce the risks that their operations have on personal privacy. They are currently recommended but not required. They tend to be used when rolling out new technology.

The Regulation will make it a legal requirement to undertake a PIA in certain cases.

It's time to think twice and assess the impact of your operations...

What do you need to know?

- A PIA will need to be carried out before the start of any project or processing activity which poses a "high risk" to an individual's privacy (e.g. an activity which uses information relating to health or race, or which involves large scale surveillance).

- Any PIA which is carried out should include: a description of the processing activity and its purpose; an assessment of the need for the processing; a summary of the risks identified and the measures to be taken to reduce them; and details of any security measures which have been taken to protect personal data.

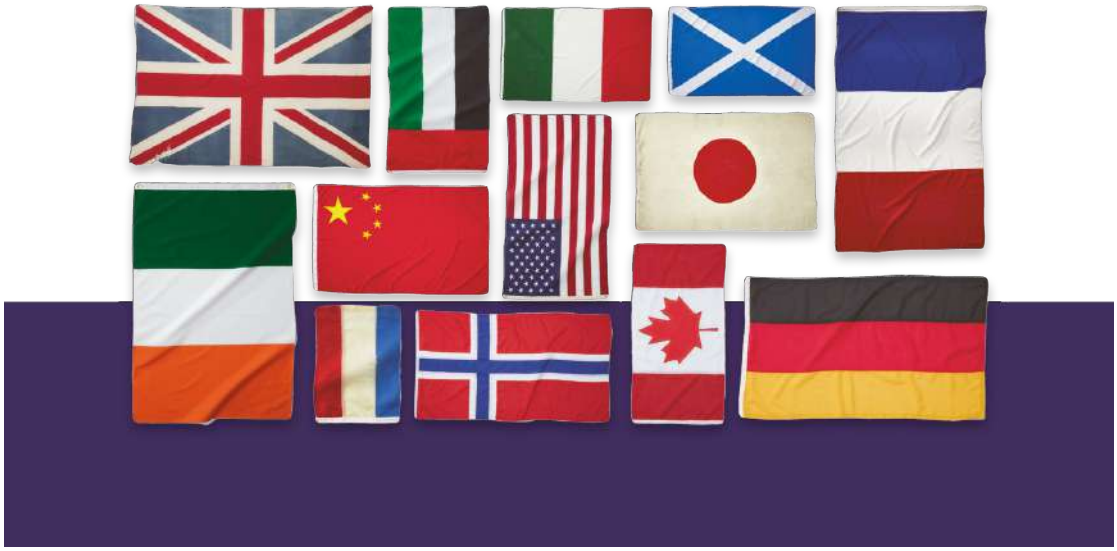
- The ICO will need to be consulted if a PIA reveals a high level of risk which cannot be reduced.

- Monitor the publication of any industry-specific codes of practice on running PIAs and adopt any guidance which they provide.

What do you need to do?

- Incorporate PIAs into your project development processes and other procedures.

SHARING HERE / SHARING THERE / SHARING EVERYWHERE



One of 2015's biggest privacy news stories was the finding that the certification mechanism that US based companies can use to demonstrate that they have internal controls in place to manage use of personal data is invalid. The scheme - known as "Safe Harbour" - was abandoned and has been replaced by the "Privacy Shield".

The repercussions of this finding will be felt for some time to come with other challenges ongoing and this has the potential to impact other mechanisms for handling personal data internationally. In light of this, before you start sharing data internationally, you should think carefully...

What do you need to know?

- The basic rule is that you can only transfer personal data outwith the European Economic Area to a country that provides an "adequate" level of protection for use of such data. Safe Harbour was one mechanism to enable this.

- A number of options in addition to Safe Harbour exist to demonstrate adequacy or to side step the requirement. Safe Harbour was only relevant for US companies who had self certified. The Privacy Shield is up and running now.

- The other options remain largely unchanged in the Regulation but external political pressure may influence data transfers.

- The other options include, entering into model contracts between data exporters and importers; establishing within a company a system of internal processes / procedures for intra-group transfers; or seeking consent from those affected.

What do you need to do?

- Map out where your data is going. Mapping should include data flows internally within your organisation but also externally to service providers, customers and any other third parties.

- Consider what mechanism you rely on. Layering different options to comply may be prudent.

GOODBYE DATA PROTECTION?

Following the Brexit decision in June 2016 there has been some uncertainty over whether the UK would adopt the Regulation.

The recent Queen's Speech in June 2017 has helped to clarify the position, and the UK government has confirmed that new data protection legislation will be introduced in the UK to implement the Regulation.

While this decision will likely mean changes to the way UK organisations handle personal data, it will ensure that data can continue to flow between the UK and the rest of the EU unhindered and uninterrupted in both the short and the long term.

In the short term, adopting the Regulation will go towards satisfying the UK's obligations while it remains a member of the EU. The UK will still be an EU Member State once the Regulation comes into force in May 2018 and as a result it will be required to comply with the terms of the Regulation along with its other EU counterparts.

While in the longer term, implementing the Regulation will ensure the UK is well-placed to continue lawfully sharing personal data internationally and with the rest of the EU post-Brexit. The law prevents organisations from sharing data to countries outside of the European Economic Area (the EU Member States plus Norway, Iceland and Liechtenstein) unless adequate protection is in place. If the UK falls out of the European Economic Area following Brexit, steps will need to be taken to demonstrate the "adequacy" of its data protection laws. If the Regulation was not implemented in

the UK, it could prove very difficult to meet this hurdle of adequacy which could be another roadblock to the continuing trade and the flow of data between the UK and the EU.

The decision by the UK government set out in the Queen's Speech to implement the Regulation will ensure a level playing field between the UK and the EU, in both the lead up and aftermath of Brexit, when it comes to data protection and will help support the digital economy as a result. At the same time implementing the Regulation will also help protect the rights of UK citizens by setting a "best practice" standard for UK organisations to follow when handling their personal data.

APPENDIX 1 - INFORMATION NOTICES

Under the Regulation organisations are required to supply individuals with detailed "fair processing notices" to ensure that they are made fully aware of what their personal data is being used for.

Such notices should include information on the following:

USES OF DATA

- The identity and contact details of the data controller (or its representative).
- The purpose(s) for processing the data.
- The recipient(s) of the data.
- Details of any transfer of the data outside the EU and how it will be protected.
- How long the data will be retained for (or at a minimum, the criteria which will be used to determine how long the data will be kept).
- Information on whether the data will be processed as part of an automated decision process and the consequences of that processing for the individual.

INDIVIDUAL'S RIGHTS

- Notice that the individual has the right to access the data held about them – including the right to restrict or object to the processing of any personal data held about them.
- Notice that the individual has the right to lodge a complaint about the processing of their data to a supervisory authority.
- The consequences of the individual failing to provide the data when it is a contractual or statutory requirement to do so.

In addition to these specific requirements there is also a general transparency obligation which will require organisations to include any further information concerning the processing of an individual's information which is not covered by the requirements above.

APPENDIX 2 - LAWFUL PROCESSING

The Regulation provides six grounds which give organisations a lawful basis for the processing of personal data. They are as follows:

- Consent of the data subject – the consent must be specific and limited to the specific processing purpose which is being considered. See our earlier section on this topic.

- Processing is necessary for the performance of a contract between the organisation and the data subject or for entering into a contract with the data subject.

- Processing is necessary for the organisation's compliance with a legal obligation.

- Processing is necessary to protect the vital interests of the data subject or another person.

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of an organisation's official authority.

- Processing is necessary for the purposes of legitimate interests – however, this ground can no longer be relied upon by public authorities processing data in the normal exercise of their functions.

FURTHER PROCESSING

The Regulation sets out factors to assist an organisation in determining whether a new purpose for processing is compatible with the purpose for which data was initially collected. These factors will need to be taken into account where the processing of data is not based on the data subject's consent or on matters such as safeguarding national security, defence or public security.
The factors to be considered are:

- Any link between the original purpose for which the data was collected and the proposed new purpose for processing.

- The context in which the data was collected – particularly regarding the relationship which exists between the data subject and the organisation.

- The nature of the personal data – particularly if it concerns sensitive data or data relating to criminal offences.

- The possible consequences of the proposed further processing for the data subject.

- The existence of any appropriate safeguards which could be used, such as encryption or using pseudonyms.

SENSITIVE PERSONAL DATA – SPECIAL PROCESSING GROUNDS

The Regulation provides that sensitive personal data can only be processed if at least one of the following special grounds for processing sensitive personal data applies:

- The data subject has given explicit consent to the processing of their sensitive personal data for one or more specified purposes.

- Processing is necessary for carrying out obligations or exercising rights related to employment or social security.

- Processing is necessary to protect the vital interests of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person.

- Processing is carried out by non-profit organisation with a political, philosophical, religious or trade-union aim and the processing relates solely to members or former members of that organisation.

- Processing relates to sensitive personal data which has been manifestly made public by the data subject.

- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity.

- Processing is necessary for reasons of substantial public interest.

- Processing is necessary for the purposes of preventive or occupational medicine, workplace assessments, medical diagnosis, the provision of health or social care treatment or processing is required under a contract with a health professional (who is subject to professional confidentiality).

- Processing is necessary for archiving purposes in the public interest, scientific and historical research or statistical purposes.

APPENDIX 3 - TOP TIPS FOR CONTROLLER / PROCESSOR CONTRACTS

The Regulation prescribes a long list of matters which will need to be addressed in contracts between controllers and processors. In particular, contract will need to address the following areas:

- Sufficient guarantees given to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject – this is far wider than just security undertakings as previously required under the current law;

- Sub-contracting must be consented to by the controller, and the processor must ensure sub-processors have sufficient guarantees in place to meet the requirements of the Regulation;

- Details regarding the subject matter and duration of processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller need to be included;

- Personal data may only be processed under documented instructions from the controller;

- Processors must inform the controller when they are required to process personal data due to a legal requirement unless they are preventing from doing so on grounds of public interest;

- Processor staff must be committed to obligations of confidentiality;

- Processors will need to implement security measures as required under the Regulation;

- Technical and organisational measures must be in place to respond to data subject rights;

- Assistance provisions should be included to support the controller with their security obligations, including: notifying breaches without undue delay, assisting with communication of breaches to those affected, and assisting with PIAs / prior consultations with data subjects;

- At the choice of the controller, processors must delete or return personal data after the end of the provision of services. This extends to copies of data unless local law requires retention; and

- Processors need to supply information to the controller on request to demonstrate the processor's compliance with their obligations and must allow for audits and inspections by the controller.

NOTES

DATA PROTECTION TEAM SHEET

We are available to assist with all aspects of data protection compliance. We'd love to hear from you!

Callum Sinclair
Partner
callum.sinclair@burnesspaull.com
+44 (0)141 273 6882
+44 (0)7391 405 414

Callum is a Partner and Head of the Technology group. He has worked in the field of information and communications technology law for over 15 years and has a life-long passion for technology. He specialises in a broad range of technology and sourcing projects for clients, principally in the financial services, utilities and public sectors (including those operating under the EU regulated procurement rules). This includes ICT procurement and sourcing, cloud and agile deals, technology partner arrangements, multi-sourcing & SIAM/Towers, networks deals and AD/AM, amongst others.

David Goodbrand
Partner
david.goodbrand@burnesspaull.com
+44 (0)131 473 6125
+44 (0)7802 933 272

David is a partner with over 15 years' experience. He specialises in advising on: outsourcing; IT procurement; IP protection and licensing; software licensing; commercial contracts; e-commerce; data protection and the use of information and Freedom of Information. David provides advice to clients in a broad range of sectors including: public sector, financial services, technology and the media.

Burness Paull

Aberdeen
Edinburgh
Glasgow

Aberdeen:
Union Plaza
1 Union Wynd
AB10 1DQ
T +44 (0)1224 621621
F +44 (0)1224 627437

Edinburgh:
50 Lothian Road
Festival Square
EH3 9WJ
T +44 (0)131 473 6000
F +44 (0)131 473 6006

Glasgow:
120 Bothwell Street
G2 7JL
T +44 (0)141 248 4933
F +44 (0)141 204 1601