Get ready | An essential guide to the General Data Protection Regulation

Using this guide

European data protection laws are being significantly overhauled. A new European General Data Protection Regulation, which will replace national data protection laws across Europe is now in force. Organisations have until 25 May 2018 to fully implement the new regime.

In this guide we give an overview of the key areas of the Regulation relevant to businesses and set out our tips on preparing for the changes.

Planning for Brexit

The Regulation is a piece of European legislation, which begs the question, what will happen to data protection in the UK in light of Brexit? There are a number of factors that need to be considered:

- Given the implementation date of 25 May 2018, the Regulation will come into force across Europe before the UK has exited the European Union. In view of this fact, the UK Government and the UK Information Commissioner have confirmed that UK organisations will have to comply directly with the Regulation until the date of exit.
- Post-Brexit, the Regulation will continue to be relevant in the UK, not least because any organisation offering goods or services into the EU will be caught by the scope of the Regulation (see paragraph 1.2).
- Multi-national organisations will find that their EU affiliates will have to comply with the Regulation, making it a practical challenge for the associated UK entity to implement different data protection regimes.
- Even UK-based organisations without an international presence may find themselves having to continue to comply indirectly with the Regulation post-Brexit. Any revised UK data protection regime will most likely incorporate key aspects of the Regulation in order to facilitate data flows with EU-based organisations.

Businesses cannot therefore ignore the requirements of the new Regulation in the hope that Brexit will mean that they do not have to comply. Steps need to be taken to ensure compliance by the 25 May 2018 deadline and organisations complying with the Regulation will be best placed to comply with any UK replacement legislation that may be adopted in due course.

Contents

1 Scope, lawful processing and consent

What is changing?

1.1 Harmonisation

The Regulation applies in all Member States so there will be no implementing legislation at national level to bring it into effect. For businesses that operate across multiple jurisdictions this harmonisation is welcome. But, there are still a number of areas where Member States can bring in their own additional legislation to specify further requirements or exemptions.

There are also procedures for more harmonisation amongst national regulators to ensure a consistent approach to enforcing the new rules.

1.2 Territory

When offering services to European consumers, non-European organisations will have to play by the European rules and adhere to the same level of protection of personal data. Any non-EU controller or processor which:

- offers goods or services to EU residents; or
- monitors the behaviour of EU residents

will be subject to the new law. Article 27 of the Regulation requires such controllers and processors to appoint an EU representative. This is unless the processing is occasional and does not include processing, on a large scale, of special categories of data or processing of data relating to criminal convictions and offences. Public authorities and bodies are exempt from this obligation.

1.3 Expansion to processors (Articles 28 to 31)

For the first time, the Regulation will introduce obligations not just on data controllers but also on data processors. These are entities that process personal data on behalf of data controllers but do not determine the purpose or means of the processing.

Compliance

Under the Data Protection Act 1998 (DPA) the data controller is already obliged to ensure that any third party data processors have appropriate security measures in place to protect any personal data they process on the data controller's behalf. These obligations are expanded under Article 28 of the Regulation. Controllers must now only use processors which take such security measures and which also comply with all other requirements of the Regulation.

Written contract

Article 28 provides that any agreement relating to processing will be governed by a contract or 'other legal act' setting out the subject matter and duration of the processing. This contract must include certain obligations, such as to process personal data only on the instructions of the controller and to assist the controller with complying with its data security obligations. The Regulation also includes an additional requirement that processors must not appoint sub-processors without the controller's consent and that contracts between processors and sub-processors should flow down all data protection obligations in the contract between the controller and the processor.

Records

Processors must maintain a record of all personal data and processing activities for which they are responsible.

This represents a significant conceptual change in placing obligations on processors for the first time, but does not relieve data controllers of any of their own obligations. Instead, more obligations are placed on data controllers to ensure that their processing contracts comply with the requirements of the Regulation.

These changes will have an effect on contract negotiations between data controllers and any data processor(s) they engage with. As data processors will be subject to their own liability for data breaches, any business acting as a data processor may well require contractual reassurance from the data controller that none of its instructions will cause the data processor to breach its data protection obligations.

Data processors should also bear in mind that the breach notification provisions (see section 5.2) mean they will be obliged to promptly notify a data controller of any data breach suffered in relation to personal data that they have processed on behalf of that data controller. If a data processor suffers a breach that affects a large number of its customers, the burden of this notification obligation will be significant.

1.4 'Personal data' (Article 4)

Many of the core definitions from the current Data Protection Directive 1995 will remain largely unchanged (eg 'controller', 'processor' and 'processing'). But, the definition of 'personal data' has caused much debate.

The Regulation defines personal data as follows:

"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

In addition to this definition, Recital 30 aims to clarify the position in relation to online identifiers (such as IP addresses and cookies) that may leave traces which, particularly when combined with unique identifiers and other information received by servers, can be used to create profiles of individuals and identify them. Such online identifiers would fall within the definition of personal data.

Recital 26 provides that individuals should be able to exercise their rights with regard to any information which is able to identify them or single them out, even if the information is considered 'pseudonymised'. When determining if a person is actually identifiable, all the means reasonably likely to be used must be considered along with the cost and time required for identification, taking into account technological developments.

1.5 'Pseudonymous data'

Currently, national Data Protection Authorities have differing approaches to pseudonymisation and anonymous data (that is, data from which no data subjects can be identified). It is therefore difficult for organisations to understand and comply with the divergent guidelines in this area.

Rather than adopting a new category of 'pseudonymous data' (as per the European Parliament's proposal), a definition of 'pseudonymisation' has been included in the new law to describe the process of data anonymisation. In addition, Article 40 states that a code of conduct should be prepared on the application of the Regulation in relation to the pseudonymisation of personal data.

1.6 Processing conditions (Articles 6 and 9)

Article 6 provides that processing of personal data will be lawful only if and to the extent that at least one of six conditions applies. Largely, these conditions mirror the conditions currently set out in Schedule 2 of the DPA. But, there are a few areas which are changing:

Consent

A data controller will still be able to rely on the consent of the data subject to justify processing of their personal data. After much debate by the European institutions, Recital 32 provides that consent should be given by a *"**clear affirmative action** establishing a freely given, specific, informed and **unambiguous** indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement."*

Vital interests

Processing is also justified if it is necessary to protect the vital interests of the data subject, as is the position under the DPA. But, the new law extends this to include situations where processing is necessary to protect the vital interests of a person other than the data subject. This gives data controllers some more leeway when it comes to assessing whether processing is necessary, as it allows them to take into account the interests of others as well as the data subject.

Legitimate interests

The general concept of necessity for the legitimate interests of the data controller to justify processing is retained. But, the legitimate interests condition will not be available to public authorities.

'...the definition of 'personal data' has caused much debate.'

1.7 Conditions for consent (Article 7)

The Regulation sets out the following requirements for consent:

Form of consent

Clear, affirmative action is required (see section 1.6). Recital 32 provides that consent could be given by *"ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data."* Consent therefore has to be a positive indication of agreement; silence, pre-ticked boxes or inactivity will not constitute consent.

Clarity

Article 7(2) specifies that if the data subject's consent is given in the context of a declaration which contains other matters, the request for consent must be *"clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language."* If it isn't, then the consent will not be binding.

Withdrawal of consent

Article 7(3) enshrines the general principle that the data subject must be able to withdraw his or her consent at any time. The data subject must be informed, prior to giving consent, of his or her right to withdraw that consent. The Regulation also provides that it should be as easy to withdraw consent as to give it.

Limitations

When assessing whether consent has been freely given, account will be taken of whether a contract or service has been made conditional upon the data subject consenting to the processing of data, where it is not necessary for those purposes.

What does this mean in practice?

It has always been advisable for organisations which act as data controllers to ensure that all of their data protection obligations are flowed down in any supplier contracts. This ensures that third party data processors are bound by appropriate obligations, as otherwise the obligations fall solely on the data controller. With the advent of specific obligations on data processors, the regulatory burden on the parties has shifted. This is likely to result in more detailed negotiations between controllers and processors and sharing of responsibilities.

The amendments relating to processing conditions mean that data controllers will need to make sure that they know exactly which condition(s) they are relying on to legitimise each type of processing carried out for each data subject.

If controllers wish to rely on consent as a condition, any consent wording will need to be sufficiently robust to allow the data controller to show that the consent given is unambiguous and that the data subject knows exactly what he or she is consenting to. The controller will also have to inform individuals that they have the right to withdraw consent at any time.

What can you do to prepare?

- carry out a data mapping exercise to identify the categories of data that your organisation is capturing and processing and to identify all data flows;
- review all the types of processing that your organisation carries out and ensure that these can be justified by one of the processing conditions;
- ensure that the particular processing conditions relied upon are appropriately documented;
- if consent is relied on, review all relevant consent wording to ensure that it adequately explains what processing will be carried out and that the data subject's consent is validly obtained.

2 Individuals' rights

What is changing?

2.1 Privacy notices (Articles 12 to 14)

Under the current law there is a requirement that data controllers must be transparent with data subjects as to what information is collected, how it is used and with whom it is shared; hence the need for privacy notices or privacy policies informing the data subject of this. The Regulation introduces far stricter minimum information requirements.

Clear information

The Regulation requires that all information that must be provided to the data subject (see 'Minimum level of information' below) must be provided in an intelligible form, using clear and plain language. This links in to the concept of "unambiguous consent"; what is important is that the data subject knows exactly what he or she is consenting to. For this to be the case, the data subject must be fully informed of what will happen to his or her personal data once it is in the hands of the data controller.

Minimum level of information

Article 13 provides that the following information should be provided, at the point when personal data is collected:

- the identity and contact details of the data controller and the data protection officer, if applicable;
- the purposes for which the data will be processed as well as the legal basis for processing;
- where processing is justified on the basis of legitimate interests, what those legitimate interests are;
- the recipients of the data;
- whether data will be transferred to a third country or international organisation;
- the period for which data will be stored;
- the existence of the rights to rectification, erasure and to object;
- the right to withdraw consent;
- the right to complain to a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract; and
- the existence of any automated decision making, including profiling (see section 2.3).

2.2 Rights of data subjects (Articles 15 to 22)

The Regulation significantly enhances the rights of individuals:

Right of access

Not only will data subjects be entitled to additional information under their rights of access in Article 15, but the time limit for the data controller to respond to subject access requests will be reduced from the current level of 40 days to one month.

After much discussion, organisations will no longer be able to charge a fee (other than for 'further copies'). Currently, data controllers do not need to comply with a request until they have received the fee which can give businesses some useful leeway in terms of the timescales.

Right to rectification

The data subject will have the right to obtain rectification of any personal data held by the data controller which is inaccurate, or completion of any incomplete personal data.

Right to erasure and to be forgotten

Individuals have a new right to require the data controller to erase all personal data held about him or her in certain circumstances, such as where the data is no longer necessary for the purposes for which it was collected. There are a number of exemptions to this right, for example in relation to freedom of expression and compliance with legal obligations.

Right to data portability

This is a new concept under the Regulation. Data subjects will have the right to transfer personal data from one data controller to another where processing is based on consent or necessity for the performance of a contract, or where processing is carried out by automated means.

2.3 Profiling (Article 22)

"Profiling" refers to automated processing of personal data used to evaluate personal aspects of an individual. Individuals will have a right not to be subject to a decision based solely on automated processing (including profiling) where that decision produces legal effects for that individual or significantly affects him or her. In practice, this means that a data subject can object to profiling and, unless an exemption applies, the data controller must no longer carry out profiling in respect of that data subject.

Exemptions include situations where the decision is necessary for a contract between the data subject and controller; is based on the data subject's explicit consent; or is authorised by law; provided there are sufficient safeguards to protect the data subject's rights.

What does this mean in practice?

Organisations that collect and use personal data will need to put in place more robust privacy notices than have previously been required, providing more information in a more prescribed manner. This will involve a large-scale review of all privacy notices.

Organisations should already have certain procedures in place to deal with the existing rights available to individuals, such as the right of subject access and the right to rectification.

Data controllers will need to consider whether these current procedures are up to scratch, in view of the changes. In particular, the impact of the changes to the time limits for subject access requests could be significant.

There will also need to be appropriate procedures and systems in place to support the new rights being introduced, such as the right to data portability and the rights relating to profiling.

What can you do to prepare?

- review all existing privacy notices and consider the changes that will be required to comply with the expanded requirements under the Regulation;
- review your current procedures for dealing with requests from data subjects to exercise their rights. Consider how these will need to be amended, and what additional procedures will need to be put in place to ensure compliance with the Regulation;
- check whether your existing IT systems are capable of enabling data deletion and rectification if individuals' rights are exercised. Ensure that new procurements take account of these requirements;
- take a look at all the circumstances in which you carry out any automated decision-making and consider how these decisions could be made differently in the event that an individual were to object.

'...what is important is that the data subject knows exactly what he or she is consenting to.'

3 Data Protection by design and default and accountability

What is changing?

3.1 Data Protection by design and by default (Article 25)

Data controllers are under a new obligation to undertake privacy by design and by default. Specifically, data controllers must take appropriate technical and organisational measures before processing begins to ensure that data processing meets the requirements of the Regulation and to ensure that by default only the minimum necessary level of personal data is collected.

3.2 Data Protection Impact Assessment (Article 35)

Currently, Data Protection Impact Assessments (DPIAs) are recommended as best practice by the ICO but are not mandatory. DPIAs form part of the Regulation's focus on "privacy by design", ie incorporating privacy considerations into a project right from the start. A DPIA is a mechanism which allows an organisation to consider the privacy risks associated with a particular project, come up with solutions to mitigate those risks and implement those solutions into the project from the outset.

The Regulation will requires DPIAs to be carried out where processing is likely to result in a "high risk" for the rights and freedoms of individuals. A DPIA shall "in particular" be required where there is automatic processing (including filing) and processing on a large scale of special categories of data.

3.3 Data Protection Officer (Article 37)

The Regulation will require certain organisations to designate a Data Protection Officer (DPO). The Commission's original proposals linking this to numbers of employees have not been adopted. Instead, a DPO must be appointed where:

- the processing is carried out by a public authority;
- the organisation's core activities require regular and systematic monitoring of data subjects on a large scale; or
- the organisation's core activities consist of processing on a large scale special categories of data and data relating to criminal convictions and offences.

3.4 Seals, certifications and codes of conduct (Articles 40 to 43)

Although a number of different privacy seal schemes and certifications currently exist, they are not explicitly recognised under existing legislation. The European institutions all agreed that the adoption of certification mechanisms and privacy seals should be encouraged to give data subjects confidence that accredited businesses are compliant with the Regulation.

Privacy seals

Voluntary data protection certification mechanisms, seals or marks may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors. Certification bodies must be accredited by the relevant supervisory authority and/or the National Accreditation Body.

Codes of conduct

The Regulation provides a framework for the adoption of EU-wide codes of conduct, which should hopefully provide clarity for businesses on how they can ensure compliance with the Regulation. Third parties, such as trade bodies, can oversee the operation of a code of conduct rather than just the competent supervisory authority or the Commission.

3.5 Record keeping (Article 30)

The Regulation abolishes the requirement to notify regulators of data processing activities. Instead, the onus is placed on data controllers and data processors to keep their own records of data processing activities and the measures they are taking to comply with the new law. Specifically, data controllers must keep records of the following:

- name and contact details of the data controller and the DPO;
- purposes of data processing;
- a description of the categories of data subjects and categories of personal data;
- categories of recipients;
- transfers of personal data outside the EEA and the safeguards in place to protect that data;
- data retention periods; and
- security measures.

What does this mean in practice?

Organisations will need to build data protection considerations into projects right from the start, rather than allowing them to become simply an afterthought. Many projects involving personal data will require DPIAs and businesses will need to have all necessary documentation in place to carry out and record the DPIAs.

There may be further administrative burdens for businesses in the form of having to appoint a DPO.

Procedures and systems will need to be put in place to document data processing and compliance measures.

What can you do to prepare?

- DPIAs will become compulsory where there is a 'high risk' for the rights of individuals. It is therefore a good idea to start looking now at your organisation's processes for carrying out DPIAs;
- similarly, ensuring now that projects involving a large amount of personal data always have a DPIA carried out is likely to help ensure a smoother transition when the Regulation comes into force;
- consider how you will document data processing activities across your organisation and the systems and procedures that will be required to keep records up to date.

'...data controllers must take appropriate technical and organisational measures to ensure that data processing meets the requirements of the Regulation and to ensure that by default only the minimum necessary level of personal data is collected.'

4 International data transfers

What is changing?

4.1 Cross border data transfers (Articles 44 to 50)

Under current legislation, businesses are prohibited from transferring personal data out of the EEA unless:

- the transfer is to an 'Adequate Jurisdiction' as determined by the Commission where it considers that the territory offers an adequate level of protection for personal data. This currently includes: Andorra, Argentina, Canada (for commercial entities subject to the Personal Information and Protection of Electronic Documents Act), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand and Uruguay;
- the transfer is made pursuant to a mechanism that ensures an adequate level of protection (eg Model Clauses); or
- a derogation applies (eg where the data subject has unambiguously consented to the transfer).

The Regulation preserves these restrictions and seeks to ensure that they are uniformly interpreted. At present, some regulators insist upon prior notification, but the new law makes it clear that notification or authorisation from a supervisory authority will not be required if the requirements are satisfied.

Perhaps the most significant change to the current position is the inclusion of an additional derogation, namely, that limited cross-border data transfers would be allowed on the basis of the controller's legitimate interests (provided that the controller puts adequate safeguards in place). This will make a significant difference to businesses who occasionally need to transfer data out of the EU, but for whom it is not feasible to obtain the consent of all the data subjects.

4.2 Binding corporate rules (Article 47)

Binding corporate rules (BCRs) are not explicitly recognised under current law. The Regulation will formalise BCRs as a valid data transfer mechanism and will, in principle, make their adoption a simpler task. Many Member States currently require additional regulator approval, but the Regulation will prevent further authorisation requirements.

The Regulation provides that BCRs should be available to both controllers and processors.

The Regulation stipulates that BCRs must include:

- a mechanism to make the BCRs legally binding on relevant group entities;
- a mechanism to grant enforceable rights to data subjects; and
- a document that sets out various information such as the structure of the group, the types of data transfer covered, the rights of data subjects and liability for breaches.

Since it should be easier for businesses to obtain approval of their BCRs if they comply with these requirements, it is likely that there will be an increase in the number of businesses that seek to implement BCRs once the new law is in place.

> '...this will make a significant difference to businesses who occasionally need to transfer data out of the EU'

What does this mean in practice?

The Regulation does not change a great deal about cross-border transfers in practice and the situation remains largely the same as it is under current UK law. For members of the same corporate group, cross-border transfers may become easier and less of an administrative burden with the new provisions around BCRs.

What can you do to prepare?

- review all instances where your organisation transfers personal data outside the EEA and ensure that these transfers can be justified on the basis of one of the existing justifications or derogations.

5 Breach notification, enforcement and sanctions

What is changing?

5.1 Supervisory authorities (Article 51 to 76)

Currently, each Member State has its own national data protection authority, such as the Information Commissioner's Office (ICO), which is responsible for enforcement of the Data Protection Directive as implemented in that Member State.

This concept remains broadly similar in the new law, with data protection authorities now being referred to as "Supervisory Authorities" or "SAs". There are three key changes to be aware of:

One Stop Shop

This was one of the most talked-about changes proposed by the Commission's original draft of the Regulation. It provided that, where a business has multiple branches in the EU, there would be a "lead authority" which would be the SA in the country where the business has its main establishment. This lead authority would supervise all the processing activities of that business throughout the EU. The original proposal has been watered down in the compromise text; there will still be a lead authority, but that lead authority must take into account the views of other SAs concerned and has a duty to cooperate with all other relevant SAs.

Consistency Mechanism

The Regulation incorporates a "Consistency Mechanism" to help ensure consistent application of the Regulation. Under this mechanism, all SAs are under a duty to co-operate with each other and the Commission. This includes, for example, obligations on an SA to communicate any draft data protection measures to the Commission and the European Data Protection Board (see below) before adopting that measure. It also includes obligations to consult with other relevant SAs where enforcement action affects processing in several Member States. The hope is that this will lead to a consistent approach to enforcement across the EU.

European Data Protection Board

The Regulation will replace the current Article 29 Working Party with a European Data Protection Board (EDPB) whose job will include advising the EU institutions on data protection issues, advising on enforcement of the Regulation, overseeing the Consistency Mechanism and promoting cooperation between SAs.

These changes are only likely to affect businesses that operate across several Member States. For those businesses which only process personal data in one Member State, the relationship with the SA in that Member State will remain much the same as it is now without the need for input from other SAs. But, for businesses with establishments in several Member States, the main interaction will be with one SA which may be in a different Member State from the particular branch of the business concerned.

5.2 Data breach reporting (Articles 33 and 34)

The new law will introduce mandatory notification of data breaches to the SA (in the UK, the ICO) and the data subject him/herself in certain circumstances.

Notification to the SA

The Regulation provides that data breaches should be notified to the regulator unless they are unlikely to result in a *"risk"* for the rights and freedoms of individuals.

Notification to the data subject

A data breach should also be notified to the data subject if there is a "high risk" to the rights and freedoms of the data subject.

5.3 Enforcement, sanctions and penalties (Articles 77 to 84)

The Regulation includes a number of significant changes in this area.

Fines

One of the headline changes, and potentially the one that has been of most concern to businesses in the UK since the first draft of the Regulation was released, is the substantial increase in the maximum level of fine it is possible to impose. As the law stands, each Member State can impose its own maximum level of fine. Currently in the UK, the maximum fine possible for a breach of data protection legislation is £500,000 for severe breaches.

The new maximum level has varied considerably throughout the drafts. The Regulation now confirms that the new maximum level of fine is the greater of €20 million or 4% of total worldwide annual turnover. The potential financial risks will no doubt inform compliance decisions going forward.

Enforcement powers

SAs will be given far wider-ranging enforcement powers than under the current law. For example, SAs may able to audit organisations to ensure they are complying with their obligations, compel organisations to provide information regarding data protection compliance and impose a ban on processing.

Judicial remedies

Currently, the circumstances in which a data protection authority, in a particular Member State, must take action to investigate and enforce a breach vary across Member States. In the UK, the ICO is not currently obliged to investigate all complaints received. The Regulation introduces a right for individuals to obtain a judicial remedy requiring an SA to investigate a particular complaint. An individual would also, under the Regulation, be entitled to a judicial remedy against a binding decision made by a SA, as well as against a data controller or data processor itself in respect of data processing that infringes the Regulation.

Up until now, some businesses may not have considered non-compliance with data protection to be a serious risk. All of the above demonstrates how important data protection compliance will be to avoid severe sanctions which could have serious financial and reputational effects on a business.

What does this mean in practice?

Mandatory notification of breaches is likely to introduce a significantly increased administrative burden on data controllers. They will need to make sure that all staff are trained in how to recognise a data breach and how to escalate this appropriately so that, if necessary, it can be notified within the relevant timescales.

Due to the increased sanctions, businesses will need to make sure that all employees take data protection compliance seriously as the consequences could be much more severe under the new law. There is also increased potential for reputational damage if data subjects are entitled to seek judicial remedies requiring the ICO to investigate a complaint that it might not otherwise have looked into.

What can you do to prepare?

- review all data protection policies, procedures and practices across your organisation to assess compliance with the current law and ensure that the transition into the new law is as smooth as possible;
- review existing breach management procedures and think about what needs to be changed to ensure they allow for swift escalation and potential notification;
- review current employee training on data protection and consider whether this is sufficient to enable employees to quickly identify breaches and know what steps to take in the event of a breach.

‘All of the above demonstrates how important data protection compliance will be to avoid severe sanctions which could have serious financial and reputational effects on a business.’

6 Issues that continue to be governed by national law

Whilst the main aim of the Regulation is to harmonise EU law, organisations should bear in mind that there will still be a number of areas where different requirements will apply in each Member State.

Exemptions include:

1. Data processed:
   - for the purposes of national security;
   - by a natural person in the course of a personal or household activity; and
   - for the purposes of prevention, investigation, detection or prosecution of criminal offences (Article 2(2));
2. Such exemptions and derogations as the Member States consider necessary to reconcile the right to the protection of personal data with the freedom of expression and information, including for journalistic purposes (Article 85);
3. Rules relating the processing of personal data in an employment context (Article 88); and
4. Professional secrecy laws (Article 90).

7 How we can help

TLT offers a range of services to assist businesses with getting ready for the new Regulation, including readiness reviews and a gap analysis to assess the steps required to ensure compliance with the new requirements.

For more information, please contact:

Alison Deighton | Partner and head of Data Protection & Privacy

Alison advises a wide range of businesses and public sector clients on all aspects of information law. Alison has extensive experience advising clients on data protection compliance issues, including drafting privacy notices and policies, delivering training, advising on international data transfers, advising on marketing compliance issues, dealing with ICO investigations, conducting audits, managing data breach incidents and advising on data sharing arrangements. Alison also has significant experience advising organisations on GDPR implementation requirements, assisting with data mapping exercises, updating policies and procedures and drafting contractual clauses to comply with the new regime.

She also advises on freedom of information issues, including protecting information provided to public authorities, making freedom of information requests and the application of exemptions.

She is a member of the National Association of Data Protection Officers and the International Association of Privacy Professionals.

T 0333 006 0160 | alison.deighton@TLTsolicitors.com

Jenai Nissim | Legal Director

Jenai advises on the running of data protection compliance programmes, advising UK and US businesses on European privacy requirements, negotiating multi-national data transfer agreements, undertaking data protection privacy impact assessments, handling breach notifications and investigations, undertaking data protection audits and providing data protection training. She has also been instrumental in establishing and leading an enterprise wide compliance project and gap analysis of the General Data Protection Regulation (GDPR), identifying key changes and impacts to business processes and procedures.

Jenai is a member of the International Association of Privacy Professionals and holds the IAPP/EU and CIPM qualification. She also holds the PDP Practitioners Certificate in Data Protection and the ICA Certificate in Compliance.

T 0333 006 1033 | jenai.nissim@TLTsolicitors.com

Emma Davies | Associate

Emma advises on data protection issues arising out of both domestic and international commercial arrangements.

She has assisted on large outsourcing projects for PLCs involving the transfer of employee data, including HR and payroll functions and occupational health and safety services. Emma has drafted privacy policies and privacy notices, assisted clients carrying out subject access requests and has reviewed and amended data protection policies for employee handbooks. Emma is also experienced in carrying out data protection audits and advising companies on strategies to achieve data protection compliance across numerous business functions.

T 0333 006 1095 | emma.davies@TLTsolicitors.com

Emma Fox | Solicitor

Emma advises on a wide range of data protection, cyber security and e-privacy issues for many different clients. Emma's experience includes dealing with data subject access requests, advising on data protection compliance, dealing with data protection breaches and advising on cookies compliance and appeals against ICO monetary penalties.

Emma also regularly advises clients on the policies and procedures required to ensure GDPR compliance. Emma has been involved in conducting a number of data protection audits and building compliance programmes for clients in preparation for GDPR. She regularly provides data protection and e-privacy training to a range of organisations.

As part of her training Emma completed a part-time secondment to a client during which she advised in particular on data protection issues.

T 0333 006 0915 | emma.fox@TLTsolicitors.com

Laura Johnson | Solicitor

Laura advises on privacy policy strategies and general data protection compliance issues where she prepares policies, other documentation and data sharing provisions. She also has experience in advising on cookies and marketing compliance issues.

Laura regularly presents on GDPR compliance to a range of organisations and has undertaken gap analysis of current data protection provisions in contracts to ensure they are compliant with GDPR requirements.

Laura has recently completed a secondment to Home Retail Group during which she assisted with the Group's data protection audit.

T 0333 006 0575 | laura.johnson@TLTsolicitors.com

Rolla Rostam | Solicitor

Rolla is a solicitor in the General Commercial team with a wide range of experience giving practical advice in a variety of commercial matters from advising on intra-group arrangements and supply contracts to sponsorships, collaborations and cross-border transactions. Rolla's previous in-house experience means that she not only understands the commercial needs of a business but is able to give pragmatic legal advice.

Rolla also reviews, prepares and delivers training on a number of regulatory compliance and governance issues such as data protection and privacy, including compliance with new the General Data Protection Regulation.

T 0333 006 1076 | rolla.rostam@TLTsolicitors.com

Join our GDPR Practical Thinktank

We have set up General Data Protection Regulation (GDPR) Practical Thinktank to provide support and develop best practice solutions for senior in-house lawyers at major UK companies to use when implementing the new regulation. We meet every quarter at our London office (near St Paul's). If you would like to join this group, please get in touch with Alison Deighton.

tltsolicitors.com/contact

Belfast | Bristol | Edinburgh | Glasgow | London | Manchester | Piraeus