



DLA PIPER

A GUIDE TO THE GENERAL DATA PROTECTION REGULATION

For in-house lawyers, Data Protection Officers, and specialists in compliance and privacy protection

CONTENTS

5 INTRODUCTION

6 KEY FACTS

7 SCOPE

10 FAIR PROCESSING AND INDIVIDUAL RIGHTS

14 ACCOUNTABILITY WITHIN THE ORGANISATION

16 MANAGING EXTERNAL FLOWS OF DATA

18 WORKING WITH REGULATORS



INTRODUCTION

On 4 May 2016, the text of the General Data Protection Regulation (GDPR) was finally published in the Official Journal of the European Union, concluding over four years of intensive legislative work on a new data protection legal framework for Europe.

The GDPR will be effective from 25 May 2018 when it will replace the existing EC Data Protection Directive (EC/95/46) (“**Directive**”), bringing new legal rights for individuals, extending the scope of responsibilities for data controllers and processors and enhancing the regime for enforcement to include the risk of fines at up to 4% of an organisation’s worldwide annual turnover.

DLA Piper have designed this Guide to provide in-house lawyers, Data Protection Officers and others dealing with privacy compliance issues on a day-to-day basis with an easy-reference manual to the GDPR.

The Guide presents an outline of each section of the GDPR, highlighting the key areas of reform and giving practical pointers about the tasks to take to support compliance, in six sections:

- Key facts about the GDPR
- Scope
- Fair processing and individual rights
- Accountability within the organisation
- Managing external flows of data
- Working with regulators

For ease of reference, headings within each section in the Guide are colour coded to show the degree of change from the existing regulatory regime:

- **green** denotes a requirement that is largely unchanged
- **yellow** denotes a slightly modified regulatory position
- **orange** denotes an entirely new, or substantially modified regulatory requirement.

Each section also provides a clear cross-reference to the relevant Article within the GDPR, which we suggest you consult for the authoritative legal position on any particular matter.

KEY FACTS

The General Data Protection Regulation – key facts:

- Current data protection laws will be **replaced by a new regulation** known as the General Data Protection Regulation.
- The GDPR will be legally effective from 25 May 2018 in all EU member states.
- The scale of the change anticipated is substantial, requiring **action now to get ready for compliance**.
- Organisations will need to adopt a consistent and coordinated approach to compliance across all EU operations.
- Individuals will have considerably strengthened **rights to privacy** that they can enforce directly against organisations.

Key changes include:

- a requirement to apply principles of ‘privacy by design’ and ‘privacy by default’ into the process of developing and launching new technologies, products, services, etc.;
- a new obligation to carry out privacy impact assessments;
- new rights to data portability and a right to be forgotten;
- a new requirement to notify data protection supervisory authorities if a data breach takes place;
- fines for non-compliance of up to EUR 20,000,000 or (if higher) 4% of the global annual turnover of the organisation; and
- special rules around profiling and use of children’s data.



SCOPE

Who is affected?

- The territorial application of the GDPR covers much wider scope than the Directive, applying not only to organisations established in the EU, but also:
 - EU-based entities, in relation to their activities, irrespective of whether data is processed within the EU or outside the EU; and
 - organisations from outside the EU, in relation to the offering of goods (and services) to data subjects in the EU or the monitoring of their behaviour as far as their behaviour takes place within the EU.



Art. 2, Art. 3, Art. 4 point 17, Art. 27



LIST OF TASKS

- All entities to which the GDPR will apply should conduct an analysis of the impact of the GDPR on their business activities
- Non-EU based entities should make strategic decisions on their approach to the requirements of the Regulation and designate a representative for the EU for the purposes of the Regulation. (For more information see “Representative of the controller within the EU”)

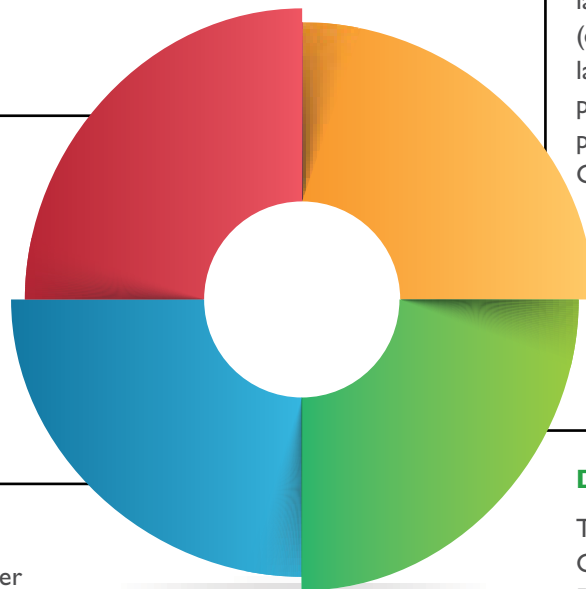
The GDPR and its legal environment

Directly effective

The GDPR takes direct legal effect in all Member States. Unlike the Directive there is no need for transposition into local national law.

Sector regulations

The GDPR allows EU member states to adopt supplementary laws in certain defined areas (e.g. in the field of employment law). These local laws can provide further regulation to the principles of protection in the GDPR.



The principle of priority

The GDPR takes precedence over any conflicting legislation that may exist in any Member State national law (including sector-related regulations).

Delegated acts

The GDPR allows the European Commission and the European Data Protection Board (EDPB) to adopt delegated and implementing acts in certain areas. The EDPB replaces the Article 29 Working Party.

Codes of conduct

- After the GDPR comes into force, expect codes of conduct and other supporting regulatory procedures to be created to supplement basic regulatory requirements in the legislation.

 Art. 40-41

Basic concepts and definitions

- The basic definitions of “processing”, “filing system”, “controller”, and “processor” are largely as in the Directive.
- The definition of “personal data” is also as in the Directive, but is supplemented to clarify that location data and online identifiers (e.g. IP addresses) also constitute personal data.
- Many new definitions have been introduced, such as “profiling”, “personal data breach”, “pseudonymisation”, “biometric data”, “data concerning health”, “group of undertakings”, and “cross-border processing”.

 Art. 4

Direct regulation of data processors

- The GDPR considerably increases the scope of regulatory compliance for organisations which process data on behalf of data controllers – so-called ‘data processors’.
- The GDPR requires data processors to implement appropriate security measures, report data breaches to the controller, maintain a register of data processing activities and seek authorisation from the controller before allowing third parties to sub-process personal data.
- Processors will be directly liable to enforcement sanctions for failure to comply with the GDPR.

 Art. 28, Art. 82-83



LIST OF TASKS

- Monitor emerging codes of conduct relevant to the particular sectors in which your business operates
- Assess the impact of those codes of conduct on your business activities



LIST OF TASKS

- Understand how the changes made to key definitions impact your processing activities

Consent is defined to mean any freely given, specific, informed and unambiguous indication of the data subject’s will by which he or she, by a statement or clear affirmative action, confirms an agreement to the processing of personal data relating to him or her.

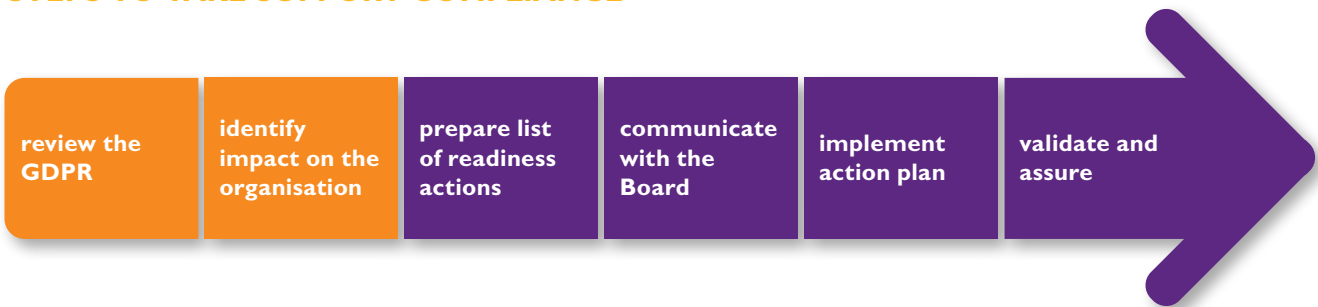


LIST OF TASKS

- If your organisation is a processor be familiar with the new obligations imposed on data processors and the new principles of liability that will apply
- In particular ensure sufficient safeguards are in place to manage compliance with the security requirements



STEPS TO TAKE SUPPORT COMPLIANCE



LIST OF TASKS

- Start taking action now to prepare for compliance, given the scale of the changes and the need to bring current data operations into line with the new requirements (e.g. with regard to obtaining consent) by 25 May 2018
- Larger organisations should consider adopting a formal change management programme, supported by step by step implementation plans



Art. 99, recital 171

FAIR PROCESSING AND INDIVIDUAL RIGHTS

Basic principles

- The basic principles requiring the processing of personal data to be for fair and lawful purposes remain largely as is within the Directive but are expanded in certain key aspects. For example, the principle of transparency is significantly strengthened so that controllers must provide much more detailed information about how data are processed, what grounds are being used to justify fair processing and what rights individuals have to access, delete and port data, and object to processing.
- A new principle of data minimisation is included – requiring the level and type of data being processed in each case to be limited to the minimum necessary.

Art. 5, Art. 11



LIST OF TASKS

- Review and evaluate the data processing procedures currently in place in the context of the revised basic principles
- Where necessary, update relevant policies to ensure that they comply with the basic principles

The grounds for fair processing

- There are far-reaching changes to the basis on which data can be fairly processed if based on ‘consent’ or ‘legitimate interests’.
- Consent can only be relied on if it is freely given, specific, informed and supported by an unambiguous indication of agreement from the data subject.
- Broadly drafted consents will not be legitimate. Nor will situations where consent is directly linked to performance of a contract, or employment status. And in each case, the individual must be able to readily withdraw any consent previously given.
- Additional rules apply when seeking to secure consent from a child.
- If relying on legitimate interests as the basis for fair processing, note that the presumption of legitimacy may be challenged by an individual (or group of individuals), in which case the processing must stop unless the controller can show compelling grounds to continue with the processing which override the individual’s rights, or alternatively if the processing is needed to establish, exercise or defend legal claims.



LIST OF TASKS

- Conduct a review of the grounds for data processing to determine whether they can still be relied upon under the new Regulation
- Draw up new consent clauses to comply with the requirements of the Regulation
- Assess the impact of the new principles concerning the processing of children’s data on the activity of the organisation

Silence, pre-ticked boxes or inactivity will not be recognised as basis for consent.

Art. 4 point 11, Art. 6-8

Special categories of personal data

- The GDPR expands the definition of sensitive data to include new fields such as biometric data.
- The GDPR sets out new detailed rules regarding situations where data are used to undertake automated decisions impacting individuals (profiling).

Biometric data – means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprint data.



Art. 4 point 13-15, Art. 9-10, Art. 22 par. 4

Profiling

- The rules allow individuals to object to decisions that directly impact them as a result of their profiles being assessed automatically to support decisions about that individual's suitability for employment, or receipt of banking or insurance products.
- Automated decisions are allowed where necessary for the conclusion or performance of a contract with the individual, or where permitted by law or based on the express consent of the individual. In other cases extra checks and balances are needed to protect the individual's rights.



Art. 4 point 4, Art. 22



LIST OF TASKS

- Review the legal grounds relied upon to legitimise the processing of sensitive data
- Consider the impact of additional duties and restrictions on business processes and procedures, e.g. the legal grounds for the processing of data concerning health, or using sensitive data for the purposes of profiling
- Monitor legislative developments that may bring additional restrictions concerning the processing of sensitive data



LIST OF TASKS

- Analyse business processes which involve profiling
- Ensure that adequate legal grounds support lawful profiling
- Comply with requirements to provide information relating to the use of automated decision making and, where applicable, introduce human intervention in the decision making process

Profiling – any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Principle of transparency

- The GDPR considerably enhances the obligation to provide information to data subjects about the manner and purposes for which personal data are to be used, and what rights they have under the GDPR.
- Privacy notices should be presented in a form that is concise, clear, easily accessible and in plain language, bearing in mind the likely recipient.

 Art. 12-14



LIST OF TASKS

- Review and, where necessary, amend privacy policies and information clauses
- Consider the possible use of graphics to help communicate privacy notices more effectively
- Ensure that if data is processed for secondary purpose(s), all necessary information is provided within the timescales set out in the Regulation
- Ensure business partners meet their own obligations to provide information to individuals if you are relying on reuse of that data
- Consider whether, under national law, any exclusions from the obligation to provide information apply

Data subjects' rights

- The GDPR expands on the existing statutory rights data subjects have (e.g. to access their data files), through a range of completely new or “refreshed” rights, as shown in the diagram below.
- Rights may be exercised freely (i.e. without charge to the data subject) and must generally be met within 30 days.
- The limited timescales for responding to requests, plus the removal of any right to charge a fee, is likely to impose a significant burden on controllers. Controllers will have to take steps to make data in their systems more easily accessible to data subjects.



LIST OF TASKS

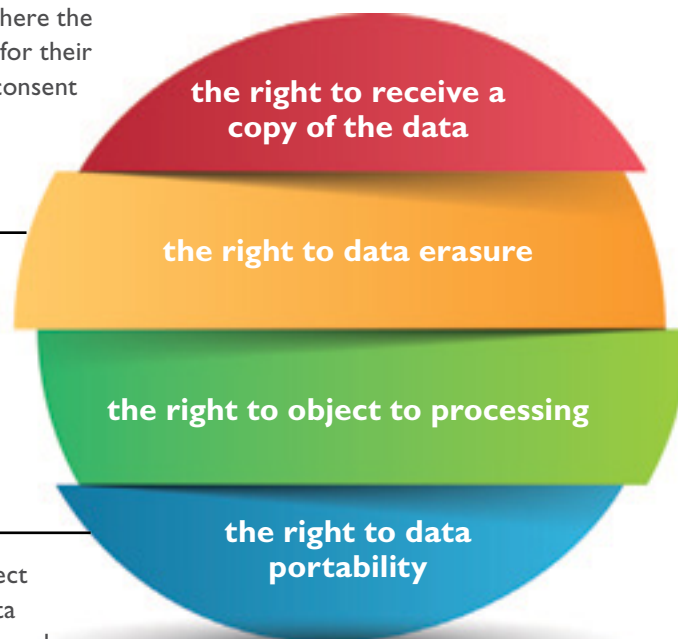
- Update internal procedures to ensure that data subjects can readily exercise the new rights available under the GDPR
- Develop standard format response letters to requests from data subjects
- Ensure appropriate safeguards are in place to prevent the unintentional disclosure of confidential business information when responding to data subject requests



Art. 4 point 3, Art. 12, Art. 15-21

The data may require the controller to erase personal data on request in a range of scenarios – e.g. where the data are no longer required for their original purpose, or where consent to processing has been withdrawn.

This right allows a data subject to receive their personal data “in a structured, commonly used and machine-readable format” and to transmit data in that format to another controller.



Individuals have the right to object to processing based on legitimate interests (including profiling), direct marketing, research and statistics. If exercised, this request must be respected unless the organisation can show there are compelling grounds to continue with the processing which overrides the individual's rights, or if the processing is required to establish, exercise or defend legal claims.

ACCOUNTABILITY WITHIN THE ORGANISATION

Principle of accountability

- The GDPR provides a new principle of accountability – requiring the controller to demonstrate active compliance with its legal responsibilities.
- This should be achieved by integrating data protection throughout the organisation’s processes and culture, including by:
 - maintaining a clear written record of all data operations which can be inspected by a regulator on demand;
 - mechanisms and procedures for monitoring and verifying compliance (e.g. regular audit);
 - measures to enhance awareness of data protection issues in the organization (e.g. training) up to senior managerial level;
 - adoption of the principle of privacy by design – ensuring data protection principles are taken into account at the early stages of designing new technologies, products and systems;
 - adoption of the principle of privacy by default – ensuring that privacy protection is adopted as a default option;
 - appointment of a Data Protection Officer (DPO) if required (see right hand column).



Art. 5 par. 2, Art. 25, Art. 30, Art. 37-39

Risk-based approach

- There is an expectation that Privacy Impact Assessments (PIA) will be undertaken for higher risk project. PIAs involve assessing potential privacy risks before starting to process data on a given project.
- Data controllers and processors have joint obligations to ensure data security (including technical safety) is appropriate at all times – taking into consideration the nature, scope, context, purposes of the processing and the related risks.



Art. 32, Art. 35-36



LIST OF TASKS

- Implement a comprehensive group wide Data Protection Compliance Programme
- Document all data processing activities
- Develop and implement an effective internal training programme
- Implement mechanisms to ensure that the principles of privacy by design and privacy by default are understood and followed for new projects/higher risk activities
- Where a DPO is appointed, take all necessary actions in connection with such appointment (e.g. ensuring that the DPO has appropriate qualifications, necessary resources, etc.)

A DPO must be appointed if:

- the organisation is processing personal data as a public entity;
- the core activities require the regular and systematic monitoring of data subjects on a large scale;
- the core activities of the organisation consist of the processing of sensitive data on a large scale.



LIST OF TASKS

- Identify the processing procedures that need to be assessed for their privacy impact and implement mechanisms to ensure that, where necessary, a PIA is carried out
- Implement organisational and technical measures to protect data, taking into consideration the level of risk, and periodically monitor such measures

Certification (marks and seals)

- The GDPR anticipates certification mechanisms which may grant special marks and seals confirming proper application of the GDPR requirements through the organisation.
- Certification will be made by appropriate certification bodies or by a competent supervisory authority.
- Obtaining a privacy certification mark allows an organisation to provide assurance that it has effective compliance with the principles in this section. It may also support transfers to a third country (see page 17).



LIST OF TASKS

- Keep an eye out for certification marks that become available and assess the organisation's eligibility to apply for certification
- Implement procedures to ensure that the adopted solutions comply with the requirements of the GDPR



Art. 24 par. 3, Art. 25 par. 3, Art. 28 par. 5, Art. 32 par. 3, Art. 42-43, Art. 46 par. 2



MANAGING EXTERNAL FLOWS OF DATA

Joint controllers

- The GDPR anticipates situations where data processing is carried out by joint controllers. In such cases the joint controllers should clearly define the allocation of responsibilities between them for key tasks such as:
 - managing the rights of data subjects;
 - providing clear information to individuals about how their data will be processed;
 - designation of a contact point for data subjects.
- Irrespective of the division of tasks and duties between joint controllers, the GDPR provides for joint and several liability vis-à-vis the data subjects.

 Art. 26



LIST OF TASKS

- Identify instances where processing is carried out by joint controllers, in particular within group companies
- Where necessary, enter into or amend contracts between joint controllers to clarify the allocation of responsibilities
- Ensure that there is a clear understanding as to who is responsible for what activities

Data processors

- The GDPR provides much more detail than the Directive regarding the arrangements for the conduct of data processing by data processors including:
 - a principle that the processor should only process data upon a documented request or instruction from the controller;
 - an obligation on the processor to maintain the confidentiality of processed data;
 - a requirement to adopt appropriate measures to protect the security of data processing;
 - an obligation to assist the controller in any cooperation required with the supervisory authority;
 - an obligation to keep an independent record of data processing activities performed on behalf of the controller.
- A data processing agreement must be in place to regulate the relationship. The terms of the agreement must include obligations related to data protection breaches, the erasure of data after the provision of services ends, and the cooperation with the data controller.



LIST OF TASKS

- Review and, where necessary, modify existing data processing agreements to ensure compliance with the new requirements
- Update related tendering documents and processes (e.g. RFP documentation, specimen letters and agreements to be used in procurement procedures) to ensure alignment with the position under the GDPR



Art. 28-31

Transfer of data to third countries

- The GDPR restates principles in the Directive governing the prohibition on the transfer of data to countries outside the EEA, unless adequate levels of protection exist in the destination country.
- In addition to the existing rules on adoption of model clauses and binding corporate rules, the GDPR anticipates other mechanisms to support lawful transfers, including:
 - codes of conduct, and
 - a new certification mechanism.
- At the same time, the significance of binding corporate rules has grown.
- The existing decisions of the Commission confirming an appropriate level of data protection in a third country and approving model clauses remain in force.

 Art. 40 par. 3, Art. 42 par. 2, Art. 44-49

Controllers not established in the EU

- If the GDPR applies to a data controller who is not established in the EU, they should designate a representative in the EU who can act on their behalf with local supervisory authorities.
- There are some exceptions to this principle – e.g. when the processing is occasional and does not involve the processing of sensitive data.

 Art. 27



LIST OF TASKS

- Review existing data transfer mechanisms
- Update the data transfer agreements in force
- Consider whether Binding Corporate Rules should be implemented
- Monitor developments regarding data transfers to the US (under the so-called Privacy Shield) and to other third countries (through the use of model clauses)



LIST OF TASKS

- Check whether it is necessary to designate a representative in the EU
- Ensure the representative is properly appointed and understands their terms of reference/responsibility

WORKING WITH REGULATORS

Cooperation with the supervisory authority

- The GDPR provides a general obligation for both controllers and processors to cooperate with the relevant supervisory authority.



LIST OF TASKS

- Develop and implement mechanisms to ensure that the obligation to cooperate with the supervisory authority is complied with in practice (e.g. by designating people in the firm who are responsible for dealing with the supervisory authority, delivering information, etc.)
- Train those who are responsible for liaising with the supervisory authority to manage those tasks effectively

Abolition of notification requirements

- The GDPR abolishes the requirement to maintain a registration of processing activities with the local supervisory authority.
- This is replaced (with certain exceptions) with an obligation to keep internal records of all data processing activities (i.e. an internal register). This must be available for inspection to the supervisory authority upon request.



LIST OF TASKS

- Develop and implement mechanisms for keeping a comprehensive internal record of data processing activities across the organisation and for disclosing the same (or request) to a supervisory authority

Consultation with the supervisory authority

- Where the results of a privacy impact assessment conclude that the proposed data processing activity would lead to a high risk to the rights and freedoms of data subjects, there is a requirement to consult with the supervisory authority. and the controller has not taken measures to mitigate that risk.



LIST OF TASKS

- Identify any data processing operations which necessitate consultation with the supervisory authority
- Develop a clean process for engaging effectively with supervisory authorities around any impact assessments requiring consultation

Notification of data breaches

- The GDPR requires the data controller to provide notification to the relevant supervisory authority of any personal data breaches.
- The notification must:
 - describe the nature of the breach;
 - state the number of the data subjects affected by the breach;
 - describe the likely consequences of the breach;
 - describe the measures taken or proposed to be taken by the controller to remedy the breach.
- There is a tight deadline for making breach notifications – the regulator should be informed within 72 hours, unless it is unlikely that the breach would result in a risk to the rights and freedoms of natural persons.
- In specific situations, the controller should also notify the data subjects affected by the breach.



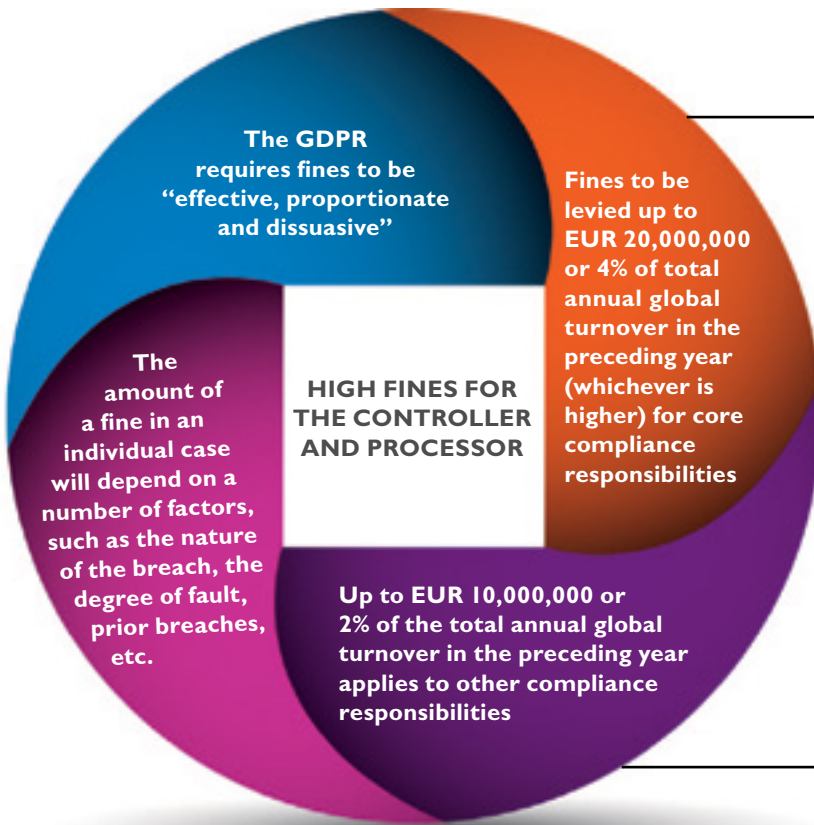
LIST OF TASKS

- Review existing procedures for dealing with data breaches
- Develop and implement a clear incident response plan, to include clear subsidiaries on notification to regulators
- Maintain a records of all incidents



Art. 33, Art. 34






- the basic principles governing data processing, including the requirements concerning the obtaining of consent (Art. 5-7 and Art. 9)
- the rights of data subjects (Art. 12-22)
- transferring personal data to third countries (Art. 44-49)
- the obligations under the national law adopted pursuant to chapter IX of the GDPR
- non-compliance with the order to restrict or suspend data processing or flow, temporarily or permanently, issued by the supervisory authority pursuant to Art. 58 par. 2 or the failure to provide access, which results in a breach of Art. 58 par. 1
- the obligations of the controller and processor referred to in Art. 8, Art. 11, Art. 25-39, Art. 42-43
- the obligations of the certification body as referred to in Art. 42-43
- the obligations of the monitoring body as referred to in Art. 41 par. 4

- In addition to exposure for regulatory fines:
 - data subjects may claim compensation from the data controller or processor for damage suffered; and
 - member states should enact local laws providing criminal sanctions for a breach of the GDPR.
- Claims or complaints may be made by not-for-profit bodies, organisations or associations.
 - on behalf of a group of data subjects.

 Art. 80, Art. 82-84



LIST OF TASKS

- Ensure the Board, and senior managerial staff understand the potential exposure to fines and other sanctions under the GDPR
- Take action to minimise potential legal liability (e.g. through the use of certification, internal audits, Compliance Gap Analysis and PIAs)
- Ensure risk arising from any data processing/ data sharing arrangements is properly managed through appropriate confidential warranties, indemnities, etc.

One-Stop-Shop Mechanism

- The One-Stop-Shop concept is a fundamental reform enshrined in the GDPR, establishing a principle that the supervisory body of **the controller's** (the processor's) **main establishment** is competent to act as lead supervisory authority for the cross-border processing carried out by that controller (processor).
- The One-Stop-Shop mechanism:
 - is intended to make it easier for controllers and processors to conduct business across EU territories;
 - requires supervisory bodies to cooperate with each other cross-border for multi-country matters;
 - will be subject to further clarification or to how the mechanism will work in practice.
- The One-Stop-Shop should lead to more joined up action by national authorities, including in the pursuit and application of enforcement where the controller is based in a number of states, or the processing operations impact entities in a number of states.

Main establishment means:

- for a controller with points of establishment in more than one Member State – the place of its central administration in the EU, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the EU and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
- for a processor with points of establishment in more than one Member State – the place of its central administration in the EU, or, if the processor has no central administration in the EU the establishment of the processor in the EU where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.

recitals 124-130, Art. 4 points 16, 28, Art. 56, Art. 60-63



LIST OF TASKS

- Identify the competent supervisory authority if the organisation's activities are conducted in more than one member state
- Understand how to interact with the lead supervisory authority and potential exposure to laws in other member states.



GLOBAL DATA PROTECTION, PRIVACY AND SECURITY

The DLA Piper Data Protection, Privacy and Security group includes over 150 lawyers worldwide.

We have built a team of privacy lawyers that are truly globally integrated, allowing us to provide advice and support in an efficient and consistent manner.

Our approach is to support clients on a 'one team' basis. Each country has its own cultural and legal context, we bring an understanding of that important local sensitivity, together with a view of overall market trends, regulations and best practice to support clients to design and implement effective privacy compliance programmes on a global scale.

For further information on how we can assist you please email us at dataprivacy@dlapiper.com.

DEDICATED EU GDPR MICROSITE

To help your organisation prepare for the new Regulation, in addition to this booklet, we have developed a dedicated microsite. The site provides key information such as what it covers, the impact it is likely to have on organisations in different sectors, actions to take now to prepare, as well as regular updates on our webinars and events on this topic.

Please visit www.dlapiper.com/dataprotection to access the microsite.

www.dlapiper.com

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication. This may qualify as "Lawyer Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2016 DLA Piper. All rights reserved. | NOV16 | 3130080