Preparing for the 2018 General Data Protection Regulations - GDPR

DCM LEARNING

Contents

Advisory

The information contained in this document is intended to provide an overview of the current data protection legislation and the major changes which will come into effect under the General Data Protection Regulations 2018. It is not intended as a comprehensive guide to these changes. Seek legal advice if you require clarification on any aspect of the regulations.

What is GDPR?

GDPR stands for General Data Protection Regulations. It is a set of articles drafted by the European Union Article 29 Working party over the past four years, designed to replace the separate pieces of legislation that each EU member state currently maintains in relation to the protection of personal data. The new regulations will come into force on the 25th May, 2018. No change in individual state legislation is required, GDPR will supersede them on that date.

As previous legislation and guidelines around data protection are now 15 years old, GDPR is designed to more effectively protect the rights of individuals with regard to their personal data, taking into account the changes in data collection and internet use in that time. In addition to clarifying and expanding the rights of EU citizens to control their personal data, it also places significant new obligations on organisations who control or process that data.

Data Protection Terms

Data

Information in a form which can be processed. It includes:

- Automated data, recorded on a computer, or with the intention of putting it on one
- Manual data, recorded on a relevant filing system, or intended to be put in one

Relevant Filing System

A system of storing information so that it can be referenced by individual criteria.

Data Processing

Collecting, organising or storing data. Retrieving, using, altering or adapting data. Combining, withholding or destroying data. Disclosing, transmitting or making data available in any way. In short, doing just about anything with the data you collect.

Personal Data

Information relating to a living individual who can be identified from that information. Can also include:

- Data that can combine with other data you hold (or can collect) to identify an individual
- Data that can be used to inform or affect decisions about an identifiable individual
- Data where the individual is the central theme of the data
- Data with the capacity to impact a specific individual in a personal, business or professional capacity

Data Subject

Any person who is the subject of personal data.

Sensitive Personal Data

Any personal data relating to:

- Racial or ethnic origin
- Religious or other beliefs
- Political affiliation or beliefs
- Physical or mental health
- Sexual orientation
- Trade union membership
- Criminal or alleged criminal history

Data Controller

Any person, organisation or group who controls the content and use of personal data.

Data Processor

A legal entity who processes data on behalf of a data controller.

Data Protection

How the privacy rights of individuals are protected with respect to their personal data.

The Eight Data Protection Principles

Obtain and process information fairly

When collecting the data, make the data subject aware of:

- The name of the data controller
- The reason the data's being collected
- Who their data may be disclosed to
- Whether questions are obligatory
- The right to access their data and rectify mistakes

Data subjects must also give consent for their data to be processed, or it can be taken as necessary for a defined number of reasons, such as for the performance of a contract the data subject has signed, or for the administration of justice.

Keep it only for one or more specified, explicit and lawful purposes

Data must only be processed for a specific, explicit and lawful purpose. A data subject has the right to ask why you're keeping their data, so data controllers must have identified the purpose of processing for all personal data they hold and confirmed that it matches the above criteria.

Use and disclose it only in ways compatible with these purposes

Personal data should only be used and shared in ways consistent with the reason it was collected. As a rule of thumb data subjects shouldn't be surprised to hear how their data is being used or shared.

Keep it safe and secure

Data controllers must take appropriate measures to ensure personal data is secure, taking into account whether it is sensitive personal data, confidential, and whether harm is likely to result from exposure. A high base standard of security is required with regard to currently available technology.

Keep it accurate, complete and up-to-date

Data must be correct and up to date. There should be systems and checks in place to ensure the accuracy of processed personal data, procedures in place to keep data current, and review and audit processes to monitor these procedures. Data held for IT backup purposes is exempt from many of these stipulations.

Ensure that it is adequate, relevant and not excessive

Only minimum amount of data required to achieve the purpose for which it was sought should be recorded.

Retain it for no longer than is necessary

Once the purpose for which data was obtained has ceased, the data must be erased. For as long as the data controller holds personal data, the full obligations of the Acts apply.

Give a copy of his/her personal data to an individual on request

On request, a data subject is entitled to:

- A copy of the data you hold about them
- Know why you keep it
- Know who you share it with
- Know the logic behind any automated decisions
- Know where the data came from

Current Irish Data Protection Legislation

The eight data protection principles are enacted in Irish Law by the Data Protection Acts 1998 and 2003. The consolidated full text of the acts can be access here:

https://www.dataprotection.ie/docs/DATA-PROTECTION-ACT-1988-REVISED-Updated-to-14-October-2014/1469.htm

The Irish Data Protection Commissioner (www.dataprotection.ie) is the supervisory authority for enforcing data protection in Ireland. They currently have limited powers, including:

- The Commissioner's power to obtain information
- The Commissioner's power to enforce compliance with the Act
- The Commissioner's power to prohibit overseas transfer of personal data
- The powers of "authorised officers" to enter and examine premises
- Appeals to the Court against the Commissioner's powers or decisions
- Prosecution of offences under the Data Protection Acts and S.I. 336 of 2011.
- Codes of Practice.

Note that their punitive powers mainly involve bringing prosecutions in relation to breaches in the Act, and where possible they enforce compliance rather than punishing breaches of the legislation. This has the capacity to change significantly with the introduction of GDPR.

GDPR – Changes and Impact

Retention and expansion of the eight data protection principles

The eight principles are retained and expanded upon with GDPR. The right of access to personal data is no longer a specific principle, but is retained and covered separately in the regulations

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

The concept of accountability is a significant new addition that imposes additional obligations on data controllers and processors.

Demonstrating Accountability

While data controllers and processors no longer need to register their activities with a supervisory authority, they are now required to be able to demonstrate, on request, their compliance with GDPR regulations This can be done by:

- Maintaining details of how data is acquired and processed
- Being able to provide such details to the supervisory authority on request
- Being able to demonstrate that consent was requested and received
- Maintaining records of measures taken to address non-compliance
- Reviewing your data protection policies to ensure that they clearly demonstrate compliance

In practice, for large organisations with large volumes of personal data, this may represent a significant obligation. Depending on how well they currently organise and map their data, including entry and exit points, data flows within the organisation and security and access rights at each point, substantial work may be required to enable the organisation to demonstrate compliance.

One-Stop-Shop

Organisations will now be able to deal with a single supervisory data protection authority, based on where the organisation has its 'main establishment'. Multinational organisations will have to decide where their main establishment is, ideally based on where the majority of decisions regarding the processing of personal data are made.

Data subjects will still be able to make complaints to their local supervisory authority, so the organisation will also have to identify 'concerned authorities' in the regions they operate in, as these may still have limited power over the organisation.

Previously each EEA member state's data protection authority would be responsible for entities within its jurisdiction. The one-stop-shop changes will require much closer co-operation between the supervisory authorities in each state.

Data Processors and GDPR

Data processors face new restrictions and obligations under GDPR. Previously they were only liable for personal data processing to the extent of their contract terms with the data processor. They now fall under the direct scrutiny of the supervisory authority, who can impose fines and enforce regulations. They can also be claimed against directly for data breaches. Specific obligations under GDPR include:

- Obtaining data controller permission before using any sub-contracted data processors
- Processing data only in accordance with controller instructions
- Maintaining data processing records and making same available to the supervisory authority
- Taking appropriate security measures and notifying the controller of any breaches
- Complying with overseas data transfer rules
- Possibly appointing a data protection officer (Article 37)

Definition of Personal Data

The definition of personal data has been extended to take account of internet technologies, and now expressly includes:

- Identification numbers
- Location data
- Online identifiers, such as IP address and cookie information, where they can be combined with other data to identify the individual

The definition of sensitive personal data has been extended to include:

- Genetic data, such as chromosomal or DNA samples
- Biometric data, such as fingerprints or voice or facial recognition data

The additional of online identifiers may require a close look at data to identify where it can be combined to identify an individual. The reclassification of genetic and biometric data will impose significant security obligations on current controllers of such data.

Additional requirements have also been imposed for the processing of children's data. Age verification and explicit guardian consent are now required, along with age-appropriate warnings where data is being collected.

Changes to consent for data collection

Consent to collection and processing of data must now involve affirmative action. Automatic opt-in, pre-ticked boxes or inactivity are no longer acceptable means of acquiring consent from data subjects.

Consent is defined as:

"Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

In addition to specifically opting-in to processing, the data subject must be advised of the reasons their data will be processed, including 'legitimate interests' processing. Legitimate interests include:

- Prevention of fraud
- Direct marketing
- Ensuring security
- Reporting possible criminal acts
- Necessary transmission of data within an organisation

Privacy by Design, Privacy by Default

Privacy by design and default is a new concept that data controllers and processors are required to embed into their organisational processes, projects and changes.

- Organisations should embed data privacy into their operational processes
- Use appropriate technical and organisational measures to ensure privacy
- Employ pseudonymisation – the renaming of identifying data fields in databases
- Implement data minimisation – by default collecting only directly relevant data
- Security should be fundamental to database design and data processing
- Data should only be processed for the specific purpose it was obtained
- Access to the data should be controlled and limited
- Retrieval, erasure and portability measures be included in data processing design

In this regard, the organisation should take into account:

- The state of the art – the current best practices and technologies
- The cost of implementation
- The nature, scope, context and purpose of processing
- The risk to individuals' rights from processing

Privacy Impact Assessments

PIAs are obligatory impact assessments that must be undertaken at the early stages of any organisational changes involving 'high risk' to the data rights of individuals, but only where the organisation or change involves:

- Large-scale processing of sensitive data
- Large-scale monitoring of a public area
- Processing of data related to criminal convictions

The Data Protection Commissioner is to produce guidelines for the requirements surrounding PIAs.

Data Protection Officers

The Data Protection Office is a new mandatory organisational appointment required where:

- The organisation is a public body
- The organisation's core activities relate to large-scale processing of sensitive data or data relating to criminal convictions
- The organisation's core activities require systematic monitoring of data subjects on a large scale

The terms of a data protection officer's appointment are specified by the regulations. They will:

- Inform and advise colleagues on their data protection obligations
- Monitor the organisation's GDPR compliance and policies
- Provide advice regarding privacy impact assessments
- Act as a point of contact with the data protection authority
- Co-operate with the data protection authority

They must:

- have "expert knowledge of data protection law"…
- …but don't have to have a specific qualification
- be adequately resourced and trained
- report directly to the highest level of management
- not receive instruction in the exercise of their tasks…
- …or be penalised or dismissed for the exercise of their tasks

Data Breach Reporting

The requirements for reporting breaches in data security have been significantly increased under GDPR. Data controllers must report data breaches to the relevant supervisory authority within 72 hours of discovering the breach, unless the breach is unlikely to result in a risk to the rights of data subjects. Data controllers must also notify data subjects affected if the breach results in "high risk" to them. If this involved disproportionate effort, for example where a large number of data subjects are affected, a public announcement may suffice instead.

Data processors must now notify data controllers when they suffer a breach, and both controllers and processors must keep records of all breaches.

New Data Subject Rights

Data subjects have a range of new rights in relation to their personal data under GDPR.

Data Erasure

Data subjects have the 'right to be forgotten' in six broad circumstances:

- Where personal data is no longer necessary in relation to the purpose for which it was collected
- Where the data subject withdraws their consent and there is no other legal ground for processing
- When the data subject objects to processing and there are no overriding legitimate grounds for processing
- The personal data has been unlawfully processed
- The personal data has to be erased to comply with a legal obligation
- Where data was collected in relation to the provision of online services for children

Data Restriction

The data subject has the right to prevent further processing of data (blocking):

- Where the data subject contests the accuracy of the data
- For unlawful processing
- Where the controller no longer needs the data, but its required by the data subject to exercise or defend a legal claim
- Where the data subject has objected to processing, pending a decision on whether the objection is valid

Data Portability

The data subject has the right to have personal data transmitted to another data controller without hindrance, where technically feasible. This is only possible in relation to data given with consent, and does not apply to data generated by the controller.

Data Profiling

Data profiling is defined as “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 or behaviour, location or movements“

The data subject has the right not to be subject to a decision based solely on automated processing, except where they explicitly agree or via contract.

Fines and Compensation Claims

Each supervisory authority now has the power to impose fines on controllers and processors for non-compliance with GDPR. This is a significant departure from previous legislation, where the Data Protection Commissioner typically enforced compliance through the threat of prosecution. The supervisory authority can now impose fines of up to €20 million, or 4% of the organisation’s total worldwide turnover. These fines can be in addition to, or instead of, corrective measures. This highlights the need for management of personal data to be addressed at the highest levels of the organisation.

Data subjects now have the right to claim non-pecuniary damages (ie. damages for distress) in respect of loss or damage resulting from data breaches. In addition to this, where non-compliance is established, the controller bears the burden of proving that they are not responsible for the events giving rise to damages. This may give rise to an increase in both the number and cost of claims resulting from data breaches.

Data Access Requests

Access request response time has been reduced to one month under GDPR. You can no longer charge for access requests, except where excessive effort is required to satisfy it. Additionally, the access request can only be refused where it is:

“manifestly unfounded or excessive, in particular because of its repetitive character.”

It is the controller’s responsibility to prove that this is the case.

GDPR specifies additional information to be provided to a data subject as part of an data access request:

- Purpose of processing, categories of personal data, recipients of the data
- The source of the information (if not collected directly from the data subject)
- Details of any automated processing, including profiling
- The data retention period, or the criteria used to determine it
- The right to complain to the supervisory authority
- The significance and consequences of any data profiling
- The safeguards in place for any data moved out of the EEA

International Data Transfers

Data transfers outside the EEA are prohibited unless the receiving country ensures appropriate safeguards. GDPR now also prohibits any non EEA court from ordering the disclosure of personal data unless under an international agreement. Existing mechanisms for data transfers have been retained and expanded upon:

BCRs (Binding Corporate Rules) are internal organisational codes of conduct the organisation agrees to be bound by in their processing of data across borders.

Model Contracts are contracts with specific provisions for data protection that has been approved by the relevant supervisory authority. Organisations can voluntarily enter into such contracts to satisfy GDPR provisions.

Approved Codes of Conduct are similar to BCRs, approved by the relevant supervisory authority.

Approved certification mechanisms – industry specific programs that would be used to satisfy GDPR data transfer requirements. The concept is still in development, with a preference for a common EU GDPR baseline certification for all contexts and sectors, which can be differentiated in its application by different certification bodies during the certification process.

Preparing your Organisation for GDPR

Step 1: Inventory your data (not just personal data)

- Why do you hold it?
- Where and how is it stored?
- Do you still need it?
- Is it adequately secured?

Step 2: document how data flows through your organisation

- Where does it enter and leave the organisation?
- Who can access it at each point?
- Where is it shared, and is it done so overseas?
- Can anonymous data be combined to identify individuals?

Step 3: Train staff in new requirements

- Developers in Privacy by Design, By Default, anonymisation
- Customer facing staff in access request changes
- Sales staff in data collection requirements
- Operations staff in data retention, portability and erasure
- Management in the large-scale impact of GDPR

Step 4: Review procedures

- Review existing processing procedures to account for new data subject rights -
- Portability, erasure, retention, excessive information
- Review data subject access procedures to comply with new requirements

Step 5: Examine the basis on which you collect data

- Amend consent procedures to comply with expanded requirements
- Examine any existing 'legitimate interests' reasons for collecting and processing
- Any personal data collected should have consent, a legal requirement or a legitimate organisational interest in line with GDPR descriptions of same

Step 6: Review your consent procedures

- Review how you seek, obtain and record consent
- Is consent explicit?
- Are the reasons for collection provided?
- Is there a procedure in place for withdrawing consent?
- And for subsequently blocking/erasing data?

Step 7: Create data breach reporting procedures

- Designed with the 72 hour timeframe in mind
- Multiple points of contact for each element
- Reporting accuracy depends on how comprehensive your data inventories and data flows are
- Ensure all staff are aware of timeframes and penalties

Step 8: Determine if you are required to appoint a Data Protection Officer

- Examine your legal requirements
- Decide if you should appoint one as a best practice measure
- Be aware of the terms of appointment – expertise, reporting, resources
- Internal appointment or external hire?

Step 9: Modify project and change management procedures:

- Train project managers in new design requirements
- Ensure privacy by design, by default can be demonstrated in the project management process
- Make staff aware of the requirements for Privacy Impact Assessments and implement procedures for carrying them out

Step 10: Identify relevant third parties

- Identify your 'main establishment' – where processing decisions are made
- Identify who your data protection supervisory authority will be
- Identify any 'concerned authorities' – other EEA areas your operate in
- Review data access and breach reporting procedures in light of this
- Identify any data processors and review contracts to comply with GDPR
- Identify any overseas data flows and review compliance instruments

Useful Resources

You can access the full text of the GDPR regulations, organised by articles and chapters here: https://gdpr-info.eu/

The Irish Data Protection Commissioner's website contains a wealth of information useful for interpreting the regulations: www.dataprotection.ie

The GDPR Portal Site: It focuses on providing data subject information, but is useful regardless: www.eugdpr.org

Most large Irish corporate law firms have produced guides or have ongoing blogs on the implications of GDPR for business. A&L Goodbody have produced a particularly comprehensive guide:

http://www.algoodbody.com/expertise/eu_general_data_protection_regulation

DCM LEARNING

Data Protection

Half Day Introduction to **GDPR**

Irish Law

The **1998 Data Protection Act** was passed by Parliament to control the way information is handled and to give legal rights to people who have information stored about them.

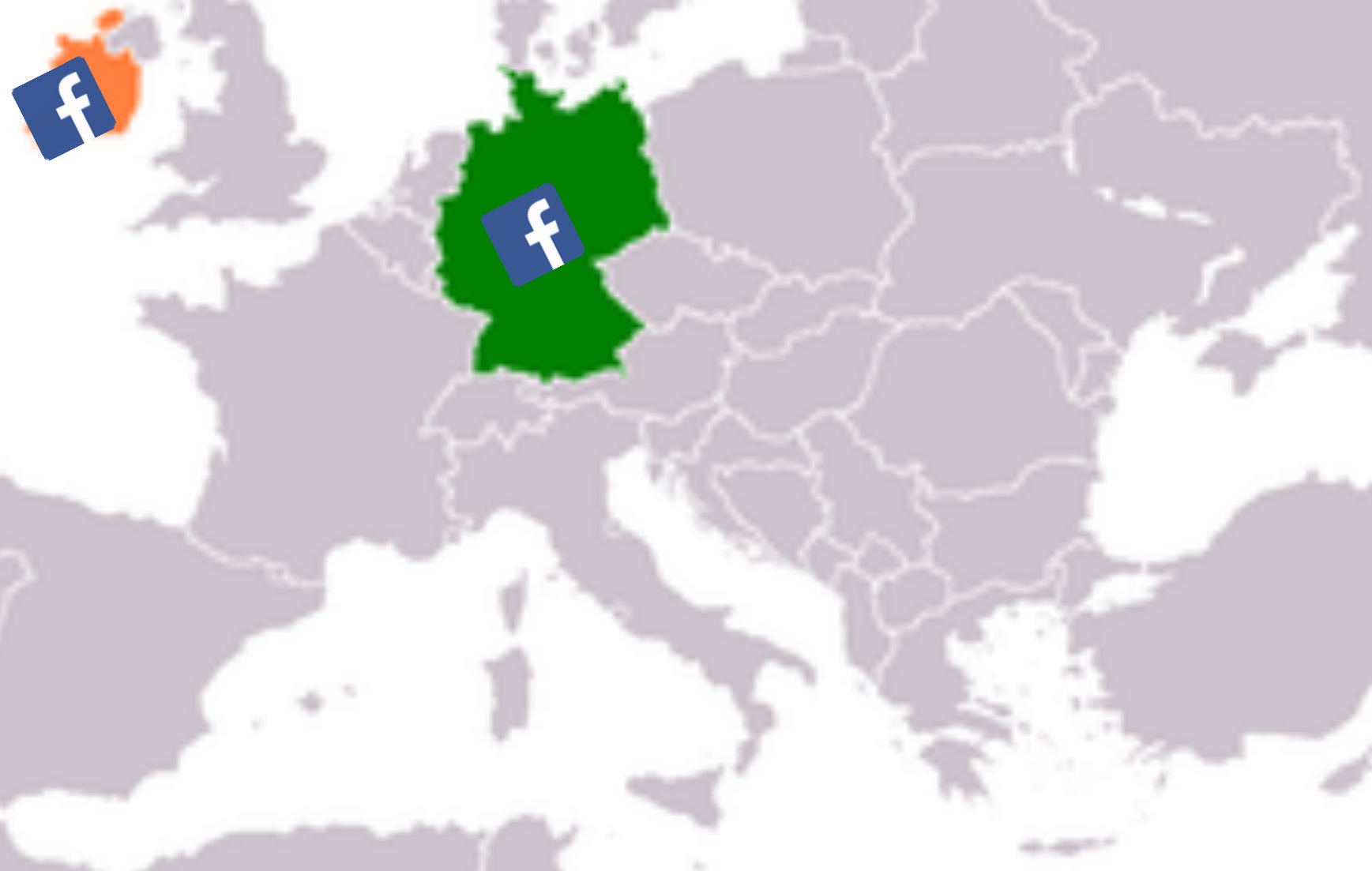
Basically it works by:

- setting up rules that people have to follow
- having a Commissioner to enforce the rules

It does not stop organisations storing and using information about people.
It just makes them follow rules.

Why do we need an update?

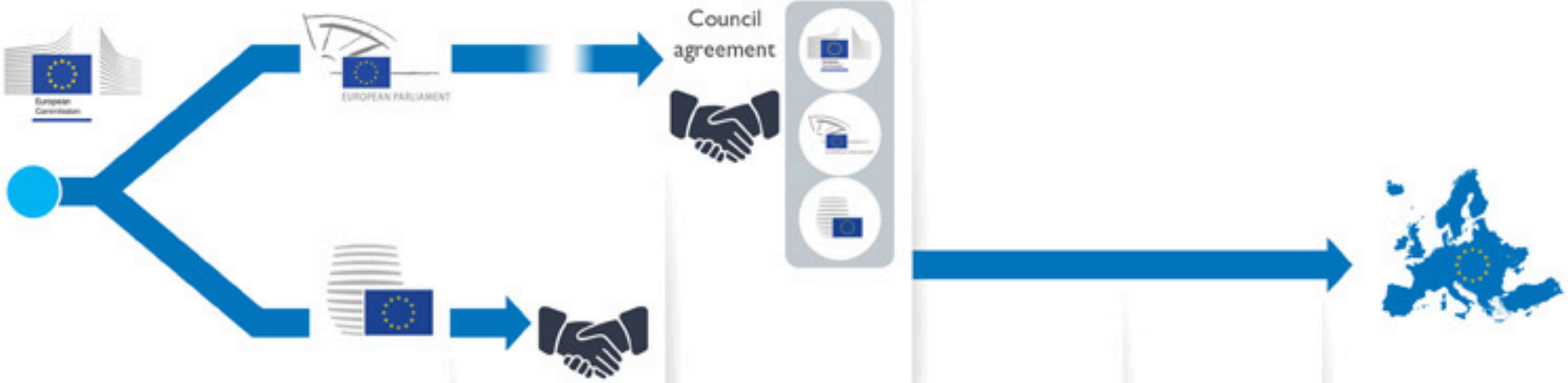
facebook



General Data Protection Regulation

(GDPR)

Overview of GDPR and how it will affect you…



European Commission publishes the legislative proposal	Separate negotiations within Council and European parliament	EP reaches agreement	Negotiations and approval among the three institutions	Adoption of the Regulation	Two years implementation phase	Regulation starts to apply
2012	SPRING 2014	2015	SPRING 2016	2016 2017		2018 May, 25th

As of TODAY
240 days
to become
compliant

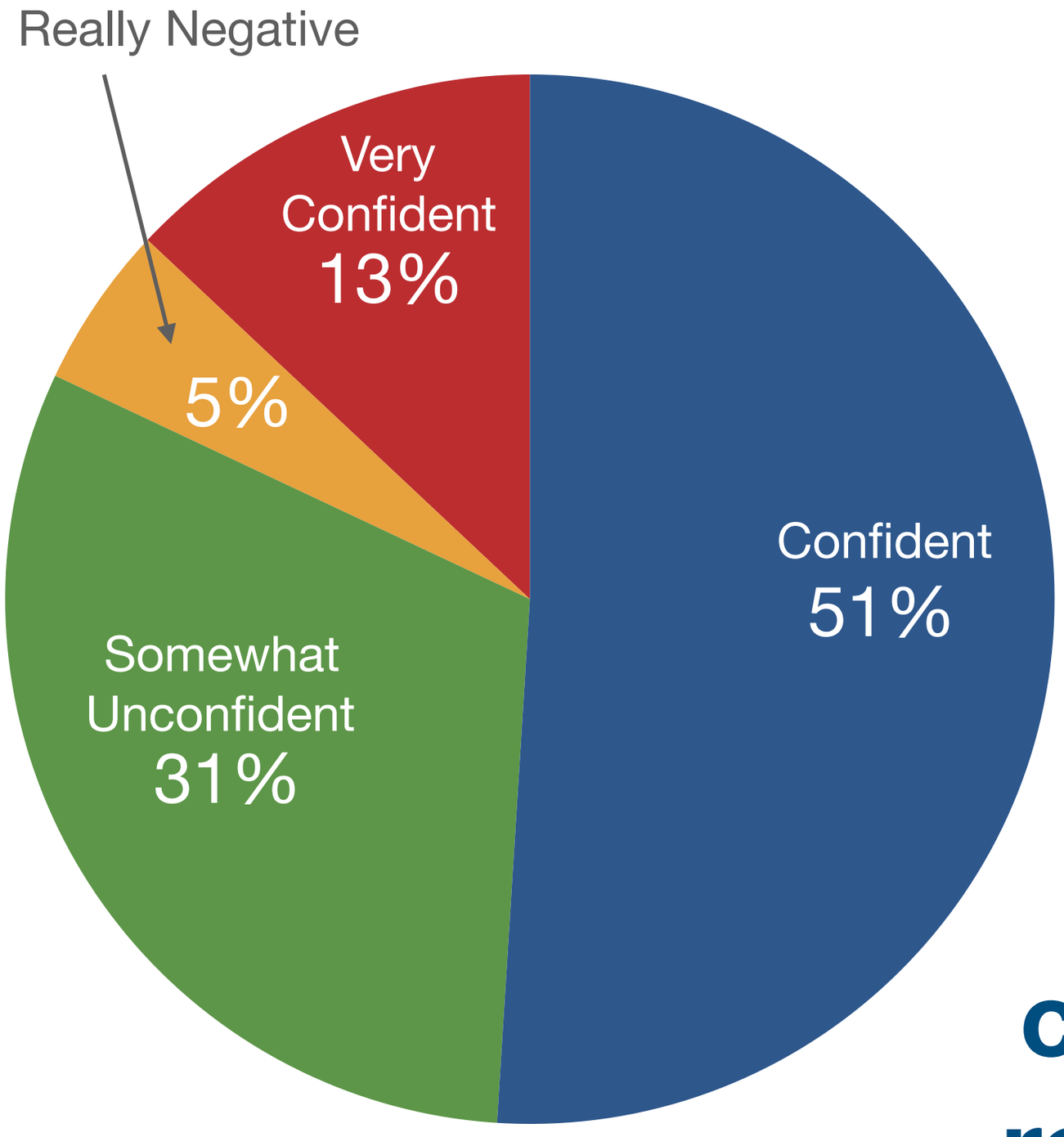
GDPR: Who must comply?

It's **GLOBAL** in reach!

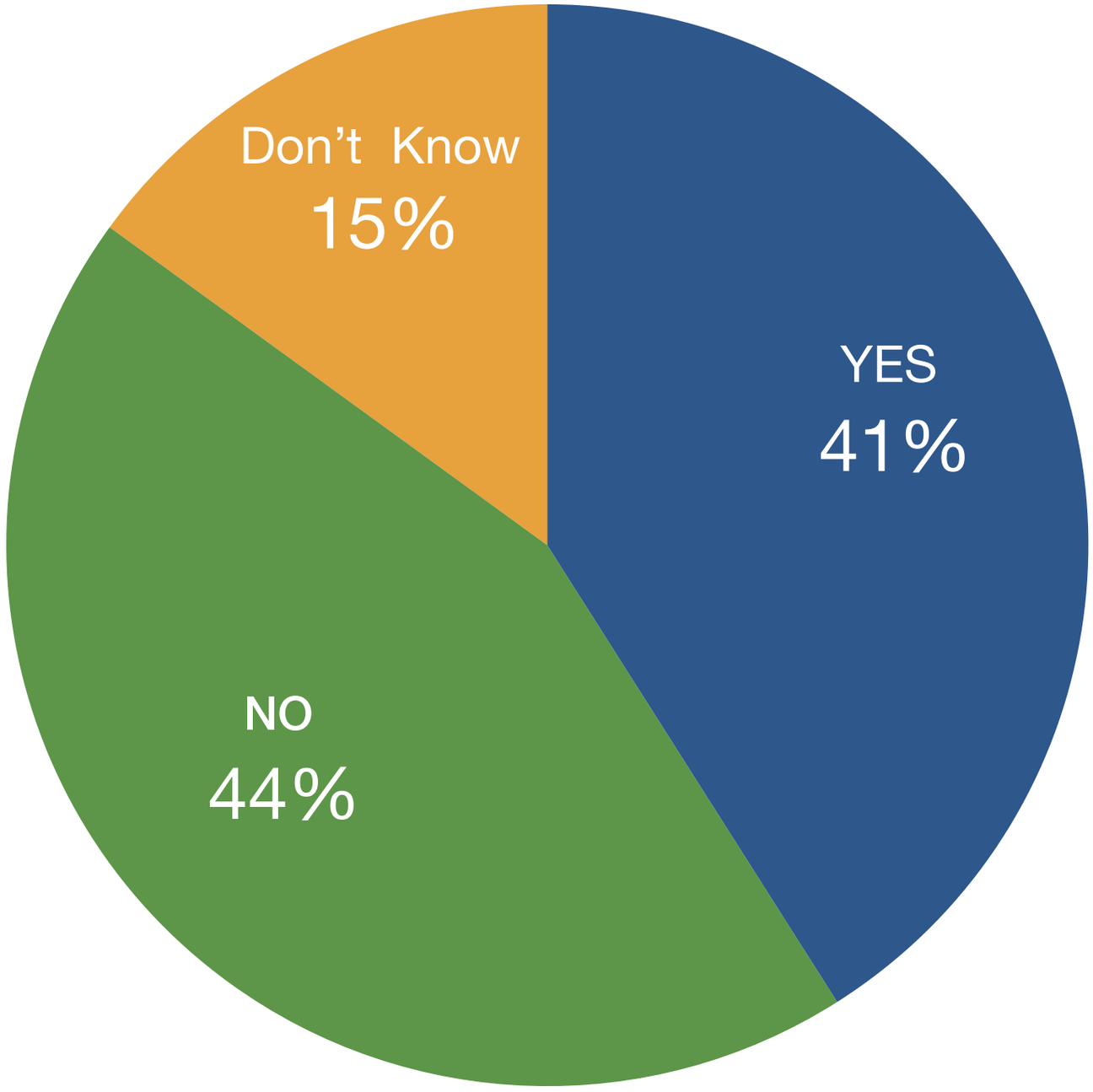
ALL organisations processing information about **European data** subjects must comply

Fines of up to **4%** of annual revenue or **20 million euro**, whichever is greater for non-compliance

Start date: **May 25th, 2018**



About a third of companies are not ready for the GDPR



More than half of companies do not have a data protection officer or don’t know they need one

Key Requirements of GDPR

Right to be forgotten
(RTBF, Article 17)

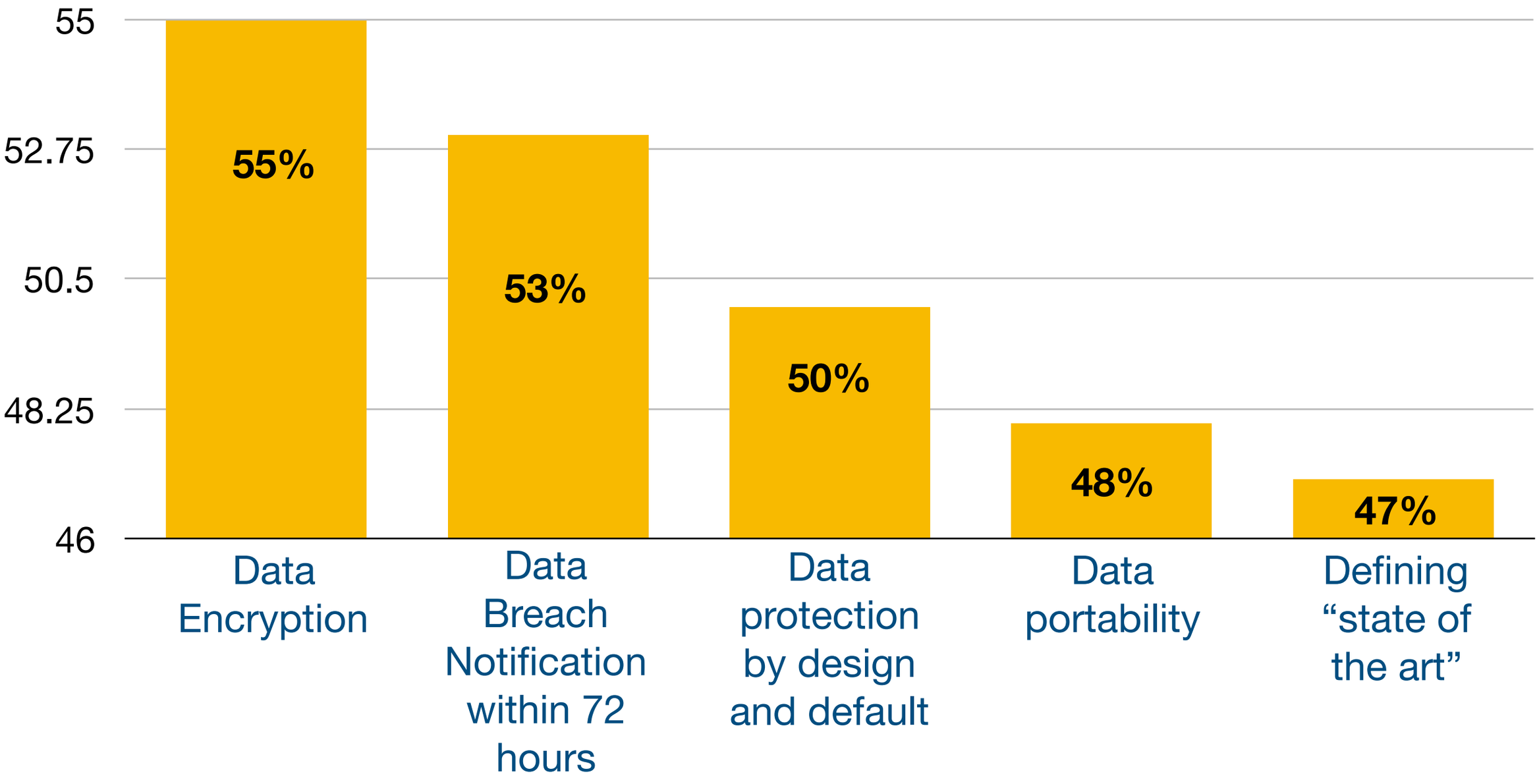
Data protection by design and default
(Article 25)

72-hour data breach notification
(Article 33 & 34)

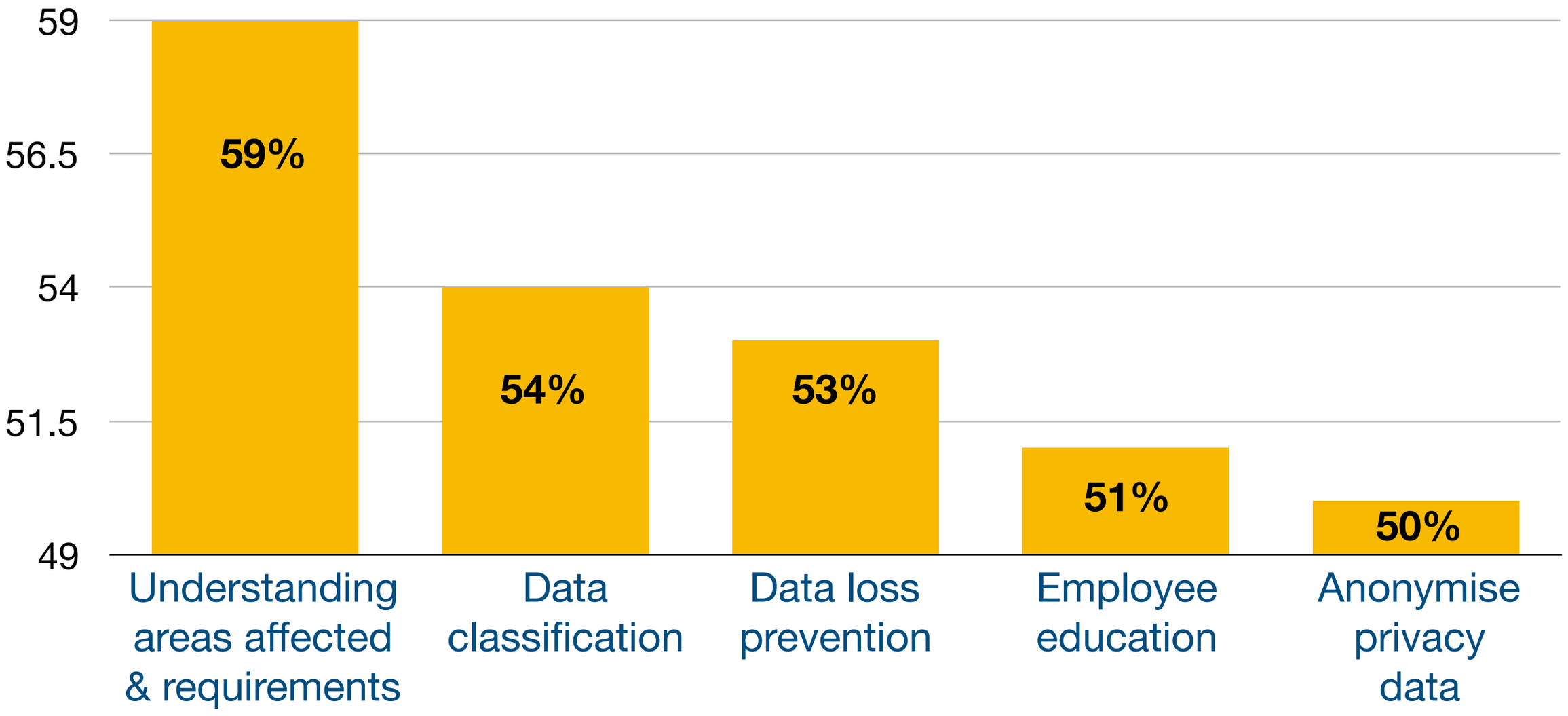
State of the art
(SOTA, Article 25 & 32)

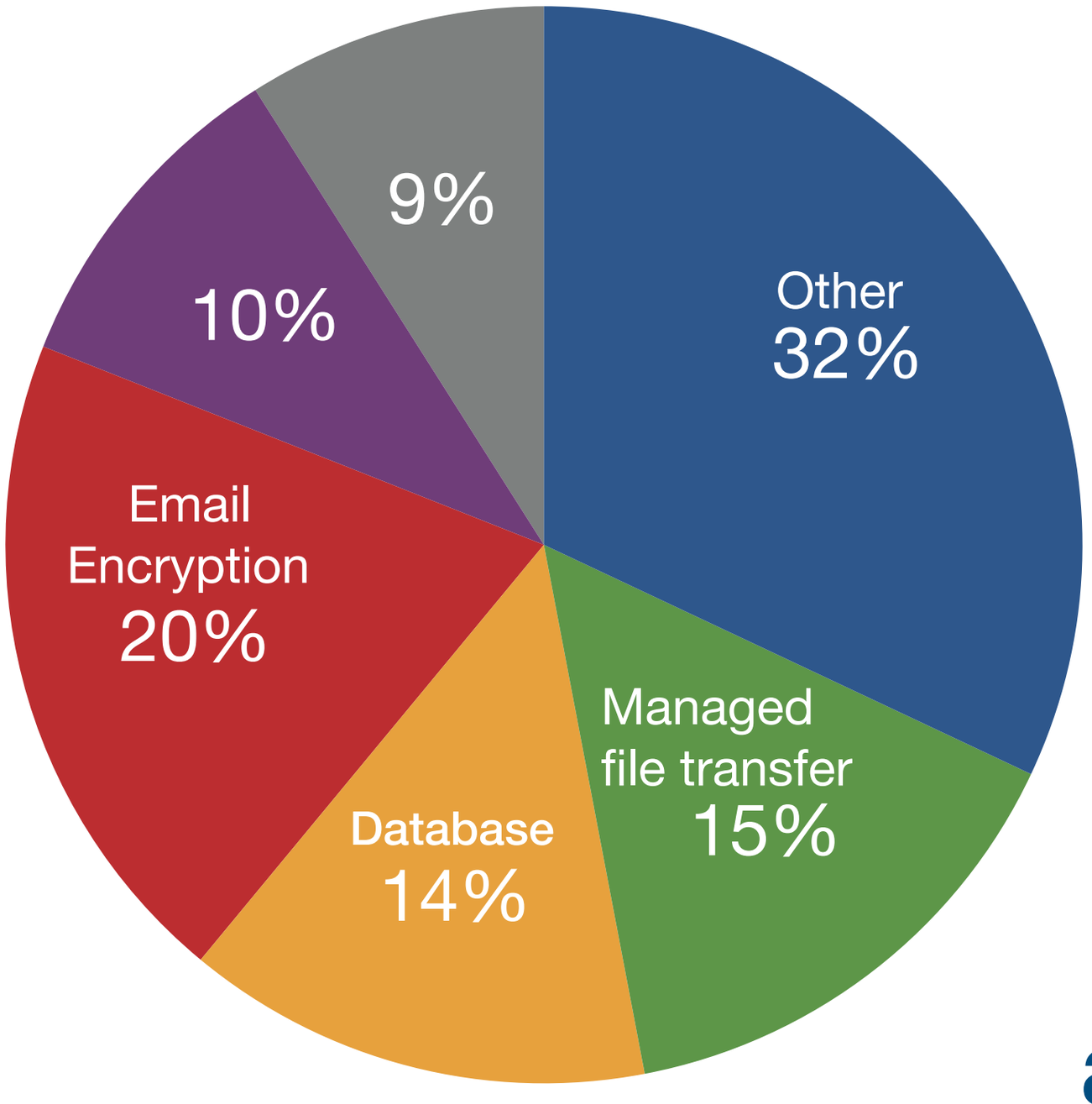
Data minimisation principle
(Article 5)

Which GDPR requirements are most challenging?



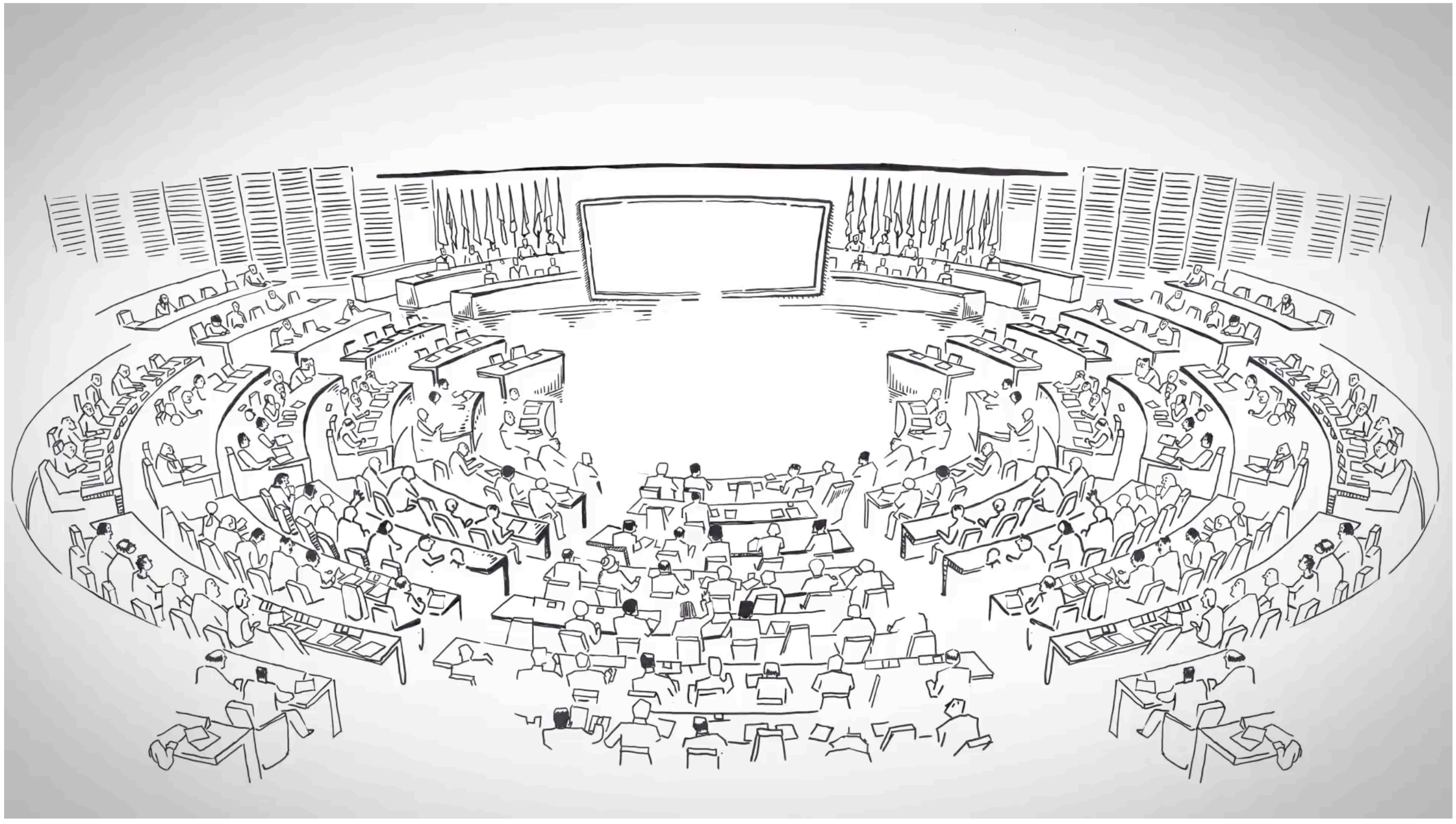
Which GDPR compliance actions are most challenging?





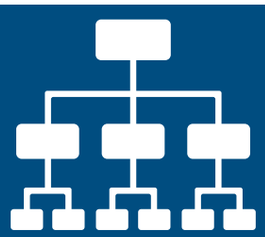
Email encryption and managed file transfer are the top two GDPR priorities

Are you ready?



GDPR: Best Practice for compliance

Set up a **cross-functional** data governance team



Launch a **data mapping and analytics** project

Use a **single platform** for data governance and policy management

Define state-of-the-art IT technologies necessary for GDPR compliance

Develop an incident response process and TEST IT!

It’s not just IT,
THINK Cross Functional

The GDPR and You

General Data Protection Regulation

An Coimisinéir Cosanta Sonraí / Data Protection Commissioner

1

Becoming Aware

Review and enhance your organisation's risk management processes – identify problem areas now.

2

Becoming Accountable

Make an inventory of all personal data you hold. Why do you hold it? Do you still need it? Is it safe?

3

Communicating with Staff and Service Users

Review all your data privacy notices and make sure you keep service users fully informed about how you use their data.

4

Personal Privacy Rights

Ensure your procedures cover all the rights individuals are entitled to, including deletion and data portability.

5

How will Access Requests change?

Plan how you will handle requests within the new timescales – requests must be dealt with within one month.

6

What we mean when we talk about a 'Legal Basis'

Are you relying on consent, legitimate interests or a legal enactment to collect and process the data? Do you meet the standards of the GDPR?

7

Using Customer Consent as grounds to process data

Review how you seek, obtain and record consent, and whether you need to make any changes to be GDPR ready.

8

Processing Children's Data

Do you have adequate systems in place to verify individual ages and gather consent from guardians?

9

Reporting Data Breaches

Are you ready for mandatory breach reporting? Make sure you have the procedures in place to detect, report and investigate a data breach.

10

Data Protection Impact Assessments (DPIA) and Data Protection by Design and Default

Data privacy needs to be at the heart of all future projects.

11

Data Protection Officers

Will you be required to designate a DPO? Make sure that it's someone who has the knowledge, support and authority to do the job effectively.

12

International Organisations and the GDPR

The GDPR includes a 'one-stop-shop' provision which will assist those data controllers whose companies operate in many member states. Identify where your Main Establishment is located in the EU in order to identify your Lead Supervisory Authority.

Data Protection Commissioner

An Coimisinéir Cosanta Sonraí

Become Aware

It is imperative that key personnel in your organisation are aware that the law is changing to the GDPR, and start to factor this into their future planning. They should start to identify areas that could cause compliance problems under the GDPR. Initially, data controllers should review and enhance their organisation's risk management processes, as implementing the GDPR could have significant implications for resources; especially for more complex organisations. Any delay in preparations may leave your organisation susceptible to compliance issues following the GDPR's introduction.

Become Accountable

Make an inventory of all personal data you hold and examine it under the following headings:

- Why are you holding it?
- How did you obtain it?
- Why was it originally gathered?
- How long will you retain it?
- How secure is it, both in terms of encryption and accessibility?
- Do you ever share it with third parties and on what basis might you do so?

This is the first step towards compliance with the GDPR's accountability principle, which requires organisations to demonstrate (and, in most cases, document) the ways in which they comply with data protection principles when transacting business. The inventory will also enable organisations to amend incorrect data or track third-party disclosures in the future, which is something that they may be required to do.

Communicating with staff and service users

Review all current data privacy notices alerting individuals to the collection of their data. Identify any gaps that exist between the level of data collection and processing your organisation engages in, and how aware you have made your customers, staff and service users of this fact. If gaps exist, set about redressing them using the criteria laid out in ‘2: Becoming Accountable’ as your guide.

Before gathering any personal data, current legislation requires that you notify your customers of your identity, your reasons for gathering the data, the use(s) it will be put to, who it will be disclosed to, and if it’s going to be transferred outside the EU.

Under the GDPR, additional information must be communicated to individuals in advance of processing, such as the legal basis for processing the data, retention periods, the right of complaint where customers are unhappy with your implementation of any of these criteria, whether their data will be subject to automated decision making and their individual rights under the GDPR. The GDPR also requires that the information be provided in concise, easy to understand and clear language.

Personal Privacy Rights

You should review your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

Rights for individuals under the GDPR include:

- subject access
- to have inaccuracies corrected
- to have information erased
- to object to direct marketing
- to restrict the processing of their information, including automated decision-making
- data portability

Personal Privacy Rights

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the Acts, but with some significant enhancements. Organisations who already apply these principles will find the transition to the GDPR less difficult.

Review your current procedures. How would your organisation react if it received a request from a data subject wishing to exercise their rights under the GDPR?

- How long to locate (and correct or delete) the data from all locations where it is stored?
- Who will make the decisions about deletion?
- Can your systems respond to the data portability provision of the GDPR, if applicable where you have to provide the data electronically and in a commonly used format?

How will access rights change?

You should review and update your procedures and plan how you will handle requests within the new timescales. (There should be no undue delay in processing an Access Request and, at the latest, they must be concluded within one month).

The rules for dealing with subject access requests will change under the GDPR. In most cases, you will not be able to charge for processing an access request, unless you can demonstrate that the cost will be excessive. The timescale for processing an access request will also shorten, dropping significantly from the current 40 day period. Organisations will have some grounds for refusing to grant an access request. Where a request is deemed manifestly unfounded or excessive, it can be refused. However, organisations will need to have clear refusal policies and procedures in place, and demonstrate why the request meets these criteria.

You will also need to provide some additional information to people making requests, such as your data retention periods and the right to have inaccurate data corrected. If your organisation handles a large number of access requests, the impact of the changes could be considerable. The logistical implications of having to deal with requests in a shorter timeframe and provide additional information will need to be factored into future planning for organisations. It could ultimately save your organisation a great deal of administrative cost if you can develop systems that allow people to access their information easily online.

What is ‘Legal Basis’

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it. This is particularly important where consent is relied upon as the sole legal basis for processing data. Under the GDPR, individuals will have a stronger right to have their data deleted where customer consent is the only justification for processing. You will have to explain your legal basis for processing personal data in your privacy notice and when you answer a subject access request.

For government departments and agencies, there has been a significant reduction in the number of legal bases they may rely on when processing data. It will no longer be possible to cite legitimate interests. Instead, there will be a general necessity to have specific legislative provisions underpinning one or more of the methods organisations use to process data. All organisations need to carefully consider how much personal data they gather, and why. If any categories can be discontinued, do so. For the data that remains, consider whether it needs to be kept in its raw format, and how quickly you can begin the process of anonymisation and pseudonymisation.

Using customer consent as grounds to process data

If you do use customer consent when you record personal data, you should review how you seek, obtain and record that consent, and whether you need to make any changes. Consent must be ‘freely given, specific, informed and unambiguous’. Essentially, your customer cannot be forced into consent, or be unaware that they are consenting to processing of their personal data. They must know exactly what they are consenting to, and there can be no doubt that they are consenting. Obtaining consent requires a positive indication of agreement – it cannot be inferred from silence, pre-ticked boxes or inactivity.

If consent is the legal basis relied upon to process personal data, you must make sure it will meet the standards required by the GDPR. If it does not, then you should amend your consent mechanisms or find an alternative legal basis. Note that consent has to be verifiable, that individuals must be informed in advance of their right to withdraw consent and that individuals generally have stronger rights where you rely on consent to process their data. The GDPR is clear that controllers must be able to demonstrate that consent was given. You should therefore review the systems you have for recording consent to ensure you have an effective audit trail.

Reporting data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Some organisations are already required to notify the DPC when they incur a personal data breach. However, the GDPR will bring in mandatory breach notifications, which will be new to many organisations. All breaches must be reported to the DPC, typically within 72 hours, unless the data was anonymised or encrypted. In practice this will mean that most data breaches must be reported to the DPC. Breaches that are likely to bring harm to an individual – such as identity theft or breach of confidentiality – must also be reported to the individuals concerned. Now is the time to assess the types of data you hold and document which ones which fall within the notification requirement in the event of a breach. Larger organisations will need to develop policies and procedures for managing data breaches, both at central or local level.

It is worth noting that a failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Data Protection Impact Assessment (DPIA) & Data protection by design and default

A DPIA is the process of systematically considering the potential impact that a project or initiative might have on the privacy of individuals. It will allow organisations to identify potential privacy issues before they arise, and come up with a way to mitigate them. A DPIA can involve discussions with relevant parties/stakeholders. Ultimately such an assessment may prove invaluable in determining the viability of future projects and initiatives. The GDPR introduces mandatory DPIAs for those oganisations involved in high-risk processing; for example where a new technology is being deployed, where a profiling operation is likely to significantly affect individuals, or where there is large scale monitoring of a publicly accessible area.

Where the DPIA indicates that the risks identified in relation to the processing of personal data cannot be fully mitigated, data controllers will be required to consult the DPC before engaging in the process. Organisations should now start to assess whether future projects will require a DPIA and, if the project calls for a DPIA, consider:

- Who will do it?
- Who else needs to be involved?
- Will the process be run centrally or locally?

It has always been good practice to adopt privacy by design as a default approach; privacy by design and the minimisation of data have always been implicit requirements of the data protection principles. However, the GDPR enshrines both the principle of ‘privacy by design’ and the principle of ‘privacy by default’ in law. This means that service settings must be automatically privacy friendly, and requires that the development of services and products takes account of privacy considerations from the outset.

DPIA's

- Under the GDPR, DPIA's will be mandatory for any new high risk processing projects.

- The DPIA process will allow you to make informed decisions about the acceptability of data protection risks, and communicate effectively with the individuals affected.

- Not all risks can be eliminated, but a DPIA can allow you to identify and mitigate against data protection risks, plan for the implementation of any solutions to those risks, and assess the viability of a project at an early stage.

- If a DPIA does not identify mitigating safeguards against residual high risks, the Data Protection Commissioner must be consulted.

- Good record keeping during the DPIA process can allow you to demonstrate compliance with the GDPR and minimise risk of a new project creating legal difficulties.

Data Protection Officer

The GDPR will require some organisations to designate a Data Protection Officer (DPO). Organisations requiring DPOs include public authorities, organisations whose activities involve the regular and systematic monitoring of data subjects on a large scale, or organisations who process what is currently known as sensitive personal data on a large scale.

The important thing is to make sure that someone in your organisation, or an external data protection advisor, takes responsibility for your data protection compliance and has the knowledge, support and authority to do so effectively.

Therefore you should consider now whether you will be required to designate a DPO and, if so, to assess whether your current approach to data protection compliance will meet the GDPR's requirements.

Types of Data

There are **distinct types of personal data**

1. **Personal data**
2. **Sensitive personal data**

*If someone who is not entitled to see these details can obtain access without permission it is **unauthorised access**.*

The 8 Principles

For the personal data that **Data Controllers** store and process:

- It must be collected and used fairly and inside the law.
- It must only be held and used for the reasons given to the approved.
- It can only be used for those registered purposes and only be disclosed to those people mentioned in the register entry.
- The information held must be adequate, relevant and not excessive when compared with the purpose stated in the register.
- It must be accurate and be kept up to date.
- It must not be kept longer than is necessary for the registered purpose.
- The information must be kept safe and secure.
- The files may not be transferred outside of the European Economic Area unless the country that the data is being sent to has a suitable data protection law. - **Now automatic data comes under GDPR!**

Data subjects rights…

1. *A Right of Subject Access*
2. *A Right of Correction*
3. *A Right to Prevent Distress*
4. *A Right to Prevent Direct Marketing*
5. *A Right to Prevent Automatic Decisions*
6. *A Right of Complaint to the Commissioner*
7. *A Right to Compensation*

Exemptions

Complete exemptions

Any personal data that is held for a **national security** reason is not covered.

Personal data held for **domestic purposes** only at home, e.g. a list of your friends' names, birthdays and addresses does not have to keep to the rules.

Partial exemptions

e.g. Revenue, school pupils, company planning documents, health notes, statistics, employer references

You need to THINK!

- Who can hear your phone call?
- Who are you really talking to?
- Do they really need to know?
- Who can see your pc screen?
- Where does waste paper end up?
- What information is on your desk or in-tray?

You should remember these points…

- Do not leave people's information out on your desk.
- Lock filing cabinets.
- Do not leave data displayed on screen, (use a screensaver?).
- Do not leave your computer logged on and unattended.
- Do not choose a password that's easy to guess.
- Do not give your password to anyone, ever.
- Never send anything by fax or e-mail that you wouldn't put on the back of a postcard.
- Do not disclose any personal information without the data subject’s consent or verifying the enquirer (e.g. phone the Garda back via the station switch board).