

INTERNAL DOCUMENT

COMPLETE GUIDE
TO
GDPR
COMPLIANCE

李申翊 · 著

The EU General Data Protection Regulation has fundamentally transformed how businesses handle personal data.

Any company that does not follow these new norms face severe fines.

Implementing such a comprehensive reform to a vast sector of the global economy has naturally had some speed bumps.

That's why we're here. This document is meant to alleviate some of those fears..

Internal Training Document

Complete Guide to GDPR Compliance

李申翊

meniny@qq.com

2.0.0, Apr. 26th, 2021

Everything You Need to Know About GDPR Compliance.

Table of Contents

1. Preface
2. What does 'GDPR Compliant' mean?
3. Data controller vs data processor: what's the difference?
 - 3.1. What is a data controller?
 - 3.2. What is a data processor?
 - 3.3. Are you a data controller or a data processor?
4. Personal Data vs. Sensitive Data: what's the difference?
 - 4.1. What is personal data?
 - 4.2. What is sensitive personal data?
 - 4.3. Getting consent
5. Lawful bases for processing
 - 5.1. Lawfulness of processing under the GDPR
 - 5.1.1. Consent
 - 5.1.2. Contractual obligations
 - 5.1.3. Legal obligations
 - 5.1.4. Vital interests
 - 5.1.5. Public interest
 - 5.1.6. Legitimate interests
6. What is Data Protection by Design and Default?
 - 6.1. What is Data Protection by Design?
 - 6.1.1. Examples of Data Protection by Design
 - 6.2. What is Data Protection by Default?
 - 6.2.1. Examples of Data Protection by Default
 - 6.2.2. Other ways you can achieve Data Protection by Default include:
7. What are the data subject rights under the GDPR?
 - 7.1. What is a data subject?
 - 7.2. The eight GDPR data subject rights
 - 7.2.1. The right to be informed
 - 7.2.2. The right of access
 - 7.2.3. The right to rectification
 - 7.2.4. The right to erasure
 - 7.2.5. The right to restrict processing
 - 7.2.6. The right to data portability
 - 7.2.7. The right to object

7.2.8. Rights related to automated decision making including profiling

8. What is a DPIA (Data Protection Impact Assessment)?

8.1. Why are DPIAs important?

8.2. Which processing activities require a DPIA?

8.2.1. What does 'high risk' mean?

Systematic and extensive profiling with significant effects

Large-scale use of sensitive information

Large-scale public monitoring

Implementing new technology

Automated decision-making

Conducting large-scale processing

Processing biometric or genetic data

Data matching

Conducting invisible processing

Tracking

Targeting children or vulnerable people

Processing that involves risk of physical harm

9. What is a Data Protection Officer?

9.1. How to become a Data Protection Officer?

9.1.1. What do Data Protection Officers do?

9.1.2. What skills and experience are required?

9.1.3. Can organisation's employee be a DPO?

9.1.4. Can organisations share a DPO?

9.1.5. Steps to becoming a Data Protection Officer

10. GDPR's requirements for an EU representative

10.1. What does an EU representative do?

10.2. What's the difference between an EU representative and a DPO?

10.3. Do all UK organisations need an EU representative?

10.4. Selecting your EU representative

11. Do I need a lot of documents to comply with the GDPR?

11.1. List of mandatory documents required by the GDPR

11.1.1. Mandatory documents for GDPR compliance

Personal Data Protection Policy (Article 24)

Privacy Notice (Articles 12, 13, and 14)

Employee Privacy Notice (Articles 12, 13 and 14)

Data Retention Policy (Articles 5, 13, 17, and 30)

Data Retention Schedule (Article 30)

Data Subject Consent Form (Articles 6, 7, and 9)

Supplier Data Processing Agreement (Articles 28, 32, and 82)

DPIA Register (Article 35)

Data Breach Response and Notification Procedure (Articles 4, 33, and 34)

Data Breach Register (Article 33)

Data Breach Notification Form to the Supervisory Authority (Article 33)

Data Breach Notification Form to Data Subjects (Article 34)

11.1.2. Documents only required under certain conditions

Data Protection Officer Job Description (Articles 37, 38, and 39)

Inventory of Processing Activities (Article 30)

Standard Contractual Clauses for the Transfer of Personal Data to Controllers (Article 46)

Standard Contractual Clauses for the Transfer of Personal Data to Processors (Article 46)

12. How to write a GDPR Data Privacy Notice?

12.1. What is a privacy notice?

12.2. How to write a privacy notice

12.2.1. Contact details

12.2.2. The types of personal data you process

12.2.3. Lawful basis for processing personal data

12.2.4. How you process personal data

12.2.5. How long you'll be keeping their data

12.2.6. Data subject rights

13. How do you write a GDPR DSAR (Data Subject Access Request) procedure?

13.1. What is a data subject access request?

13.2. Data subject access request procedures under the GDPR

13.3. What is included in a data subject access request?

13.4. Can information be redacted?

13.5. Infographic: data subject access request flowchart

13.6. Do individuals have to give a reason for a DSAR?

13.7. Does a request have to be in writing?

13.8. Can individuals submit a DSAR on behalf of someone else?

13.9. How long do organisations have to respond to a DSAR?

13.10. Who is responsible for responding to a subject access request?

- 13.11. How much can be charged for a subject access request?
- 13.12. What's the difference between a freedom of information request and a DSAR?
- 13.13. The process for handling a DSAR
 - 13.13.1. Verify the identity
 - 13.13.2. Clarify what the request is
 - 13.13.3. Is the request valid?
 - 13.13.4. Inspect the data
 - 13.13.5. Choose the format
 - 13.13.6. Add extra information
- 13.14. How to ensure data subject access request success
 - 13.14.1. Staff training
 - 13.14.2. DSAR responsibilities
 - 13.14.3. Expert advice
- 14. How to Write a GDPR Data Protection Policy?
 - 14.1. What is a data protection policy?
 - 14.2. Why do you need a GDPR data protection policy?
 - 14.3. What your data protection policy should include
- 15. How to write a GDPR data retention policy?
 - 15.1. What is a data retention policy?
 - 15.2. Aims and objectives
 - 15.3. How long can personal data be stored?
 - 15.4. What to do with data past the retention period
 - 15.5. How to create a data retention policy
- 16. How do you write a GDPR PRBN (Personal Data Breach Notification) procedure?
 - 16.1. What is a personal data breach?
 - 16.2. Personal data breach notification procedures under the GDPR
- 17. GDPR Article 30: How do you comply with?
 - 17.1. Data mapping under the EU GDPR
 - 17.2. Creating data flow maps
 - 17.2.1. Understand the information flow
 - 17.2.2. Describe the information flow
 - 17.2.3. Identify its key elements
 - 17.3. The key challenges of data mapping
 - 17.3.1. Identifying personal data
 - 17.3.2. Identifying appropriate technical and organisational safeguards

17.3.3. Understanding legal and regulatory obligations

What is the PCI DSS?

ISO 27001 definition: What is ISO 27001?

18. GDPR Article 32: Guide to the requirements

18.1. What is Article 32 of the GDPR?

18.2. Minimum compliance requirements in Article 32

18.2.1. Pseudonymising personal data

18.2.2. Measures to protect the confidentiality, integrity and availability of personal data

18.2.3. Measures to restore data in the event of a disruption

18.2.4. Regularly test the effectiveness of these measures

18.3. GDPR Article 32 checklist

19. GDPR data transfer rules

19.1. How do I know if I'm making a restricted transfer?

19.2. How to make a restricted transfer in accordance with the GDPR?

19.2.1. Is the restricted transfer covered by an 'adequacy decision'?

19.2.2. Is the restricted transfer covered by appropriate safeguards?

19.2.3. Is the restricted transfer covered by an exception?

19.3. Pseudonymisation and encryption

19.4. What about the Schrems II ruling?

20. 7 steps to highly effective GDPR compliance

20.1. Assess your current data protection measures

20.2. Identify and minimise risks that result from your data processing

20.3. Educate and empower your employees to make better decisions

20.4. Develop controls, policies and processes

20.5. Implement a DPIA

20.6. Manage and respond to DSARs

20.7. Plan, monitor and maintain a concrete GDPR compliance programme

21. 5 things HR departments need to know about data protection

21.1. Lawful basis for processing

21.2. Data subject rights

21.3. Job applications

21.4. Acceptable use

21.5. Employee monitoring

22. 72 hours and counting: Reporting Data Protection Breaches under the GDPR

- 22.1. What is a data breach?
- 22.2. When do data breaches need to be reported?
- 22.3. Be wary of overreporting
- 22.4. How to report a data breach?
- 22.5. What happens after you report an incident?
- 22.6. What happens if you don't report an incident?

23. 3 GDPR compliance tips for small businesses

- 23.1. GDPR compliance is only difficult if you don't understand what to do
 - 23.1.1. Take an online GDPR foundation training course
 - 23.1.2. Get a 'how-to' guide as a reference
 - 23.1.3. Keep an eye out for GDPR-related news.
 - 23.1.4. Teach your staff what they should and should not do
 - 23.1.5. Enrol your team on an e-learning course
 - 23.1.6. Place visual reminders in close proximity to staff
 - 23.1.7. Document everything to highlight your compliance efforts

24. Appendixes

- 24.1. Appendix A: The GDPR Compliance Quick Checklist
- 24.2. Appendix B: The GDPR Compliance Checklist
 - 24.2.1. Select Your Role
 - 24.2.2. Data
 - 24.2.3. Accountability & Management
 - 24.2.4. New Rights
 - 24.2.5. Consent
 - 24.2.6. Follow-up
 - 24.2.7. Special Cases
 - 24.2.8. User Rights
- 24.3. Appendix C: Sample DPIA Questionnaire
- 24.4. Appendix D: Privacy Policy Template
- 24.5. Appendix E: Data Protection Policy Template
- 24.6. Appendix F: GDPR Data Map Template
- 24.7. Appendix G: Records of Processing Activities for Data Controller Template
- 24.8. Appendix H: Records of Processing Activities for Data Processor Template
- 24.9. Appendix I: Categories of Personal Information

1. Preface

The EU General Data Protection Regulation (<https://gdpr-info.eu/>) has fundamentally transformed how businesses handle personal data. Any company that does not follow these new norms face severe fines, potentially up to €20 million or 4% of annual global revenue, depending on the severity and circumstances of the violation. In other words, GDPR compliance is not optional.

Implementing such a comprehensive reform to a vast sector of the global economy has naturally had some speed bumps. Several large companies, including Google and Facebook, have run afoul of GDPR guidelines. So businesses that have neither the workforce nor the funds nor the expertise of these large multinational corporations are justified in feeling some apprehension about achieving GDPR compliance.

That's why we're here. This document is meant to alleviate some of those fears.

2. What does 'GDPR Compliant' mean?

GDPR (General Data Protection Regulation) (<https://gdpr-info.eu/>) compliance is a continual process, not a one-off activity.

Your organisation must follow the rules set out in the Regulation and keep appropriate documentation that proves you're following those rules.

You must also carry out regular risk assessments to determine if your circumstances have changed, in which case you will need to update your data processing processes and documentation accordingly.

3. Data controller vs data processor: what's the difference?

The concept of data controllers and data processors has been around for years, but the roles come with clearly defined responsibilities under the GDPR (General Data Protection Regulation).

Now, we take a close look at what a data controller and processor does and how they fit into your organisation.

3.1. What is a data controller?

A data controller determines the purposes for which an organisation collects and uses personal data. They can be an individual or a group, but as long as they have the authority to decide how and why information should be processed, they are a data controller.

However, the GDPR's obligations mean that you can't just start gathering personal information. You need a lawful basis, and it's the data controller's responsibility to decide which basis applies and to document their justification.

Data controllers must also determine:

- What types of personal data to collect (names, contact information, etc.);
- Whose personal data to collect;
- Whether the information will be shared with a third party and, if so, which one(s);
- When and where data subjects' rights apply;
- How long the data will be retained; and
- Whether to make non-routine amendments to the data.

3.2. What is a data processor?

A data processor is the person or organisation that handles personal data on behalf of the controller.

In general, data processors will be expected to:

- Oversee the logistics of data processing;
- Determine how to store the collected information;

- Ensure that the information is secure;
- Determine how to transfer personal data;
- Ensure that a retention schedule is adhered to; and
- Decide how sensitive data should be disposed when it's no longer needed.

However, this isn't to say that the data processor must do exactly what the controller demands. Before processing any information, both parties must sign a contract agreeing to their responsibilities.

The contract must state that data processors may act only on the data controller's documented instructions, that they won't contract a sub-processor without prior approval, and that they will delete or return all personal data to the data controller at the end of the contract.

3.3. Are you a data controller or a data processor?

Understanding your role as either a data controller or data processor requires you to identify the differences between the two roles.

Say, for example, that you are a marketing executive at a retailer who wants to conduct a survey on shoppers' browsing habits.

That would make you a data controller. As such, you must find a data processor to conduct the survey and provide them with the necessary information to complete that task.

If you fail to do that, you've violated the GDPR and are subject to disciplinary action. The repercussions are even worse if the data processor suffers a data breach, because you'll be liable for any mistakes they make.

However, it's not always that simple. The GDPR permits two or more organisations to jointly determine the purposes and means of processing the same personal data.

Joint data controllers must agree which one will take primary responsibility for complying with the GDPR and to make this information available to individuals.

Despite that, all joint controllers have GDPR compliance responsibilities, and supervisory authorities and individuals may take action against a controller should those obligations not be met.

If you're wondering how data processors fit into this – they must only act on behalf of, and follow the instructions of, the relevant controller.

It's worth clarifying that if multiple data controllers are processing the same data but for different purposes, they are not joint controllers; they are instead two separate data controllers that happen to be performing a similar task.

4. Personal Data vs. Sensitive Data: what's the difference?

At the heart of the GDPR (General Data Protection Regulation) is the concept of 'personal data'.

But what constitutes personal data? Are names and email address classified as personal data? What about photographs and ID numbers?

And where does the related concept of 'sensitive personal data' fit in?

If you're unsure about the answers to any of these questions, keep reading. We explain everything you need to know and provide examples of personal and sensitive personal data.

4.1. What is personal data?

In the most basic terms, personal data is any piece of information that someone can use to identify, with some degree of accuracy, a living person.

For example, the email address johnsmith@companyx.com" is considered personal data, because it indicates there can only be one John Smith who works at Company X.

Likewise, your physical address or phone number is considered personal data because you can be contacted using that information.

Personal data is also classed as anything that can affirm your physical presence somewhere. For that reason, CCTV footage of you is personal data, as are fingerprints.

That sounds simple enough so far – but things are complicated when you factor in that each piece of information doesn't have to be taken on its own.

Organisations typically collect and store multiple pieces of information on data subjects, and the amassed information can be considered personal data if it can be pieced together to identify a likely data subject.

Think of it like a massive game of Guess Who?

Under certain circumstances, any of the following can be considered personal data:

- A name and surname

- A home address
- An email address
- An identification card number
- Location data
- An Internet Protocol (IP) address
- The advertising identifier of your phone

You might think that someone's name is always personal data, but as the ICO (Information Commissioner's Office) explains, it's not that simple:

“*By itself the name John Smith may not always be personal data because there are many individuals with that name. However, where the name is combined with other information (such as an address, a place of work, or a telephone number) this will usually be sufficient to clearly identify one individual.*

However, the ICO also notes that names aren't necessarily required to identify someone:

“*Simply because you do not know the name of an individual does not mean you cannot identify [them]. Many of us do not know the names of all our neighbours, but we are still able to identify them.*

4.2. What is sensitive personal data?

Sensitive personal data is a specific set of “special categories” that must be treated with extra security. This includes information pertaining to:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data; and
- Biometric data (where processed to uniquely identify someone).

Sensitive personal data should be held separately from other personal data, preferably in a locked drawer or filing cabinet.

As with personal data generally, it should only be kept on laptops or portable devices if the file has been encrypted and/or pseudonymised.

4.3. Getting consent

A common misconception about the GDPR is that all organisations need to seek consent to process personal data.

In fact, consent is only one of six lawful grounds for processing personal data, and the strict rules regarding lawful consent requests make it the least preferable option.

However, there will be times when consent is the most suitable basis, and organisations need to be aware that they need explicit consent to process sensitive personal data.

Nuances like this are common throughout the GDPR, and any organisation that hasn't taken the time to study its compliance requirements thoroughly is liable to be tripped up.

This could lead to lasting damage, such as enforcement action, regulatory fines, bad press and loss of customers.

5. Lawful bases for processing

Under the EU GDPR (General Data Protection Regulation) (<https://gdpr-info.eu/>), you need to identify a lawful basis before processing personal data. But what is a lawful basis for processing? Do you always need individuals' consent to process their data? And what exactly are 'legitimate interests'?

The GDPR defines processing as “any operation or set of operations that is performed on personal data, whether by automated means or not, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure, or destruction”.

Before you do any of these things, you need to identify a lawful basis for doing so, according to Article 6.

Except for special categories of personal data (sensitive data), which you cannot process except under certain circumstances, there are six lawful bases for processing.

These are:

- If the data subject gives their explicit consent; or if processing is necessary:
- To meet contractual obligations entered into by the data subject;
- To comply with the data controller's legal obligations;
- To protect the data subject's vital interests;
- For tasks carried out in the public interest or exercise of authority vested in the data controller; or
- For the purposes of legitimate interests pursued by the data controller.

5.1. Lawfulness of processing under the GDPR

5.1.1. Consent

Recital 32 states:

“Consent should be given by a clear affirmative act 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.

- An ‘affirmative act’ means the data subject has to opt-in – you cannot assume their consent, for example by using pre-ticked boxes on your website.
- ‘Freely given’ means the data subject has to have genuine choice: they must not suffer any detriment if they refuse consent.
- ‘Specific and informed’ means you must clearly explain what they are consenting to: a vague or incomprehensible request for consent will be invalid.

If you rely on consent, it’s essential to keep proper records, as stipulated by Article 7(1):

“*Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*”

This is particularly important because data subjects have the right to withdraw their consent at any time.

It must be as easy for them to withdraw their consent as it was to provide it in the first place.

If they do withdraw their consent, you will be obliged to erase their data “without undue delay” if they ask you to, unless you can show a lawful reason to retain it.

Many people – and organisations – focus on consent, but it’s arguably the weakest lawful basis for processing because it can be withdrawn at any time.

It’s therefore always worth determining whether another lawful basis for processing can apply.

For example, when you process staff data for payroll purposes, contractual obligations will apply, as staff will have signed a contract of employment.

5.1.2. Contractual obligations

You can rely on contractual obligations if:

- You have a contract with someone and need to process their personal data to comply with your obligations as part of that contract; or
- You don’t yet have a contract with someone, but they’ve asked you to do something as an initial step (for example, provide a quote) and you need to process their personal data to do so.

In this context, a contract doesn't have to be a formal legal document, as long as it meets the requirements of contract law. An oral statement also counts.

The processing you carry out must be necessary for the purposes of fulfilling your contractual obligations. This lawful basis will not apply if there are other ways of meeting those obligations.

If it's necessary to process sensitive data as part of a contract, you'll also need to identify a separate condition for processing that data, as set out in Article 9(2) of the GDPR, and sections 10 and 11, and Schedule 1 of the DPA (Data Protection Act) 2018.

5.1.3. Legal obligations

You can rely on legal obligations if you need to process personal data to comply with a common law or statutory obligation. (It doesn't apply to contractual obligations.) It should be clear from the law in question whether processing is necessary for compliance.

Again, record-keeping is essential: you must be able to identify the specific legal provision you're complying with, or show the guidance or advice that sets out your legal obligation.

5.1.4. Vital interests

This basis applies if it's necessary to process personal data to protect someone's life. (This applies to any life – not just the data subject's life.)

Recital 46 of the GDPR clarifies that:

“*Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis.*”

It is unlikely to apply except in cases of emergency medical treatment.

5.1.5. Public interest

If your organisation needs to process personal data “for the performance of a task carried out in the public interest” or “in the exercise of official authority” (Recital 50), you can do so using this lawful basis.

You don't need a specific statutory power to process personal data, but you must have a clear basis in law, which you must document.

The DPA 2018 clarifies that this includes processing necessary for:

- The administration of justice;
- Exercising a function of either House of Parliament;
- Exercising a function conferred on a person by an enactment or rule of law;
- Exercising a function of the Crown, a Minister of the Crown or a government department; or
- An activity that supports or promotes democratic engagement.

Data subjects' rights to erasure and data portability do not apply if you are processing on this basis. However, they do have a right to object.

5.1.6. Legitimate interests

The most flexible of the six lawful bases for processing, legitimate interests could theoretically apply to any type of processing carried out for any reasonable purpose.

Article 6(1f) states that processing is lawful if, and to the extent that:

“processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”

On the one hand, this gives you a lot of room for interpretation.

On the other, the definition is unhelpfully vague, and the burden is on you to determine whether or not your interests in processing the personal data really are legitimate.

The ICO (Information Commissioner's Office) has published a three-part test, covering purpose, necessity and balancing.

Numerous interests can be legitimate, including your interests, third parties' interests and commercial interests. These interests must be balanced against those of the data subject(s).

The GDPR mentions processing client or employee data, marketing, fraud prevention, intra-group transfers or IT security as potential legitimate interests, but this list is not exhaustive.

The important thing to consider is that ‘legitimate interests’ is most likely to be appropriate if you are using personal data in ways that the data subjects would deem reasonable and where the processing has a minimal impact on their privacy.

And, as ever with the GDPR, it’s your record-keeping that will prove essential. If you can demonstrate that you’ve carried out a full LIA (legitimate interests assessment), the supervisory authority should be satisfied.

Remember that if you use legitimate interests as your basis for processing personal information as part of your marketing activities, the data subjects’ right to object is absolute: you must stop processing if anyone objects.

You should also check your compliance with the PECR (Privacy and Electronic Communications Regulations 2003).

If you rely on legitimate interests, the right to data portability does not apply.

6. What is Data Protection by Design and Default?

Data protection by design and default is nothing new. Essentially, it's the GDPR's version of 'privacy by design'.

But while privacy by design was good practice under the Data Protection Act 1998, data protection by design and by default are legal requirements under the GDPR.

6.1. What is Data Protection by Design?

Data protection by design is ultimately an approach that ensures you 'bake in' privacy and data protection into your processing activities and business practices.

To implement data protection by design, the GDPR says that you must:

- Put in place appropriate technical and organisational measures designed to implement the data protection principles; and
- Integrate safeguards into your processing so that you meet the GDPR's requirements and protect the individual rights.

6.1.1. Examples of Data Protection by Design

An organisation that adopts data protection by design will:

- Conduct a DPIA (data protection impact assessment) when considering a new system, service, product or process that involves personal information;
- Implement technologies, processes and policies to mitigate the risks that are discovered in the DPIA;
- Write privacy notices and data protection policies in simple, easy-to-understand language; and
- Provide data subjects with the name and contact information of its DPO (Data Protection Officer) or, if it hasn't appointed one, the person responsible for data protection.

This is by no means an exhaustive list. Data protection by design is less a set of requirements as it is a general approach to GDPR compliance.

It urges organisations to look for ways to anticipate data protection and privacy issues, and prevent them.

6.2. What is Data Protection by Default?

Data protection by default requires you to ensure that you only conduct data processing activities if they are necessary to achieve a specific goal.

It links to the GDPR's principles of data minimisation and purpose limitation.

To comply with data protection by default, you must consider:

- Assuming a 'privacy-first' stance with any default settings of systems and applications;
- Ensuring you don't provide the illusion of choice to individuals relating to the data you will process;
- Refraining from processing additional data unless the individual provides their consent;
- Ensuring that personal data is not automatically made publicly available to others unless the individual decides to make it so; and
- Providing individuals with enough controls and options to exercise their rights.

6.2.1. Examples of Data Protection by Default

What data protection by default looks like will vary based on the type of data processing the organisation is conducting.

Here's an example: an organisation introduces a voice recognition system to verify users.

The technology is beneficial to both customers and the organisation, as it reduces waiting times and doesn't require the customer to have a password or other authentication details to hand.

But to use the system, the organisation must collect a recording of customers' voices, which is considered biometric (and therefore sensitive) personal data under the GDPR.

Because the organisation has an alternative, less invasive way of completing the verification process, it cannot make voice recognition the default option.

Instead, it must inform customers that it is an option and explain how they can consent to the practice.

Similar issues can be seen in any other data processing activity that isn't essential to the service being provided.

For example, social media can do lots of different things with your personal data, but many of them are

non-essential for their primary service.

The sites must therefore turn those options off automatically, and give users the choice to activate them.

6.2.2. Other ways you can achieve Data Protection by Default include:

- Avoiding misleading choices; you can't ask users to provide their consent if you are going to process their data anyway using another lawful basis;
- Ensuring that personal data isn't automatically made publicly available to others unless the data subject consents; and
- Giving individuals a simple, easy-to-access method for adjusting their privacy settings and exercising their data subject rights.

7. What are the data subject rights under the GDPR?

The EU GDPR (General Data Protection Regulation) (<https://gdpr-info.eu/>) gives individuals eight rights relating to their personal data. Organisations must let individuals know how they can exercise these rights and meet requests promptly.

Failure to do so is a violation of the GDPR and could lead to disciplinary action. But first, what is a data subject?

7.1. What is a data subject?

The term ‘data subject’ refers to any living individual whose personal data is collected, held or processed by an organisation. Personal data is any data that can be used to identify an individual, such as a name, home address or credit card number.

7.2. The eight GDPR data subject rights

7.2.1. The right to be informed

Organisations need to tell individuals what data is being collected, how it’s being used, how long it will be kept and whether it will be shared with any third parties. This information must be communicated concisely and in plain language.

7.2.2. The right of access

Individuals can submit subject access requests, which oblige organisations to provide a copy of any personal data they hold concerning the individual.

Organisations have one month to produce this information, although there are exceptions for requests that are manifestly unfounded, repetitive or excessive.

7.2.3. The right to rectification

If an individual discovers that the information an organisation holds on them is inaccurate or incomplete, they can request that it be updated. As with the right of access, organisations have one month to do this, and the same exceptions apply.

7.2.4. The right to erasure

Individuals can request that organisations erase their data in certain circumstances – for example, when the data is no longer necessary, the data was unlawfully processed, or it no longer meets the lawful ground for which it was collected.

This includes instances where the individual withdraws consent.

The right to erasure is also known as ‘the right to be forgotten’.

7.2.5. The right to restrict processing

Individuals can request that an organisation limits the way it uses personal data.

It’s an alternative to requesting the erasure of data and might be used when an individual contests the accuracy of their personal data.

An individual can also exercise this right when they no longer use the product or service for which it was originally collected, but the organisation needs it to establish, exercise or defend a legal claim.

7.2.6. The right to data portability

Individuals are permitted to obtain and reuse their personal data for their own purposes across different services. This right only applies to personal data that an individual has provided to data controllers by way of a contract or consent.

7.2.7. The right to object

Individuals can object to the processing of personal data that is collected on the grounds of legitimate interests or the performance of a task in the interest/exercise of official authority.

Organisations must stop processing information unless they can demonstrate compelling legitimate grounds for the processing that overrides the interests, rights and freedoms of the individual.

They can also refuse this right if the processing is for the establishment or exercise of defence of legal claims.

7.2.8. Rights related to automated decision making including profiling

The GDPR includes provisions for decisions made with no human involvement, such as profiling, which uses personal data to make calculated assumptions about individuals.

There are strict rules about this kind of processing, and individuals are permitted to challenge and request a review of the processing if they believe the rules aren’t being followed.

8. What is a DPIA (Data Protection Impact Assessment)?

A DPIA is a type of risk assessment. It helps you identify and minimise risks relating to personal data processing activities. DPIAs are also sometimes known as PIAs (privacy impact assessments).

The EU GDPR (General Data Protection Regulation) (<https://gdpr-info.eu/>) and DPA (Data Protection Act) 2018

([https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA-)

[MASTER-Keeling_Schedulewith_changes_highlightedV3.pdf](#))

require you to carry out a DPIA before certain types of processing. This ensures that you can mitigate data protection risks.

For instance, if processing personal information is likely to result in a high risk to data subjects' rights and freedoms, you should carry out a DPIA.

You should also conduct one when introducing new data processing processes, systems or technologies.

8.1. Why are DPIAs important?

DPIAs are a useful way of ensuring the efficiency – and cost-effectiveness – of the security measures you implement.

A risk-based approach ensures you do not waste resources attempting to mitigate threats that are unlikely to occur or will have little effect.

When required, not carrying out a DPIA could leave you open to enforcement action from the ICO (Information Commissioner's Office) – the UK's data protection authority. This could include a fine of up to 2% of your organisation's annual global turnover or €10 million – whichever is greater.

Regular data privacy impact assessments also support the GDPR's accountability principle. This helps your organisation prove its compliance with the Regulation – both to the supervisory authority and other stakeholders.

8.2. Which processing activities require a DPIA?

8.2.1. What does 'high risk' mean?

How can you identify high-risk data processing activities? Or, to be more specific, identifying potentially high-risk data processing activities, because you won't know for sure that there are information security risks until you've completed a DPIA.

You're therefore performing a broad analysis, looking for – on the one hand – which risks are acceptable – and on the other, processing activities that might endanger data subjects' rights and freedoms.

You can do this by breaking risk into its two component parts:

- Probability: the likelihood that the data processing will result in a data breach or privacy violation.
- Damage: the impact on individuals if a data breach or privacy violation occurs.

Where you set the threshold at which risk becomes 'high' is up to you, but the GDPR includes three types of data processing that meet these criteria.

Systematic and extensive profiling with significant effects

Systematic processing includes management processes that are used to observe, monitor or control data subjects.

For example, organisations might monitor an employee's browsing habits to make sure they aren't using the Internet for illicit purposes.

Likewise, a retailer might use personal data collected about an individual to provide targeted ads.

Not every instance of systematic processing requires a DPIA. That's because the processing must also be extensive (continual monitoring as opposed to occasional checks) and have significant effects (the data reveals something sensitive about the individual).

You can define 'sensitive' by assessing the damage – be it financial, reputational or emotional – that could be caused if an unauthorised party accessed the personal data.

Large-scale use of sensitive information

'Large-scale' refers to:

- A significant number of data subjects;
- A high volume of personal data; or

- Storing data for a substantial length of time.

Meanwhile, sensitive information refers to special categories of data or personal data relating to criminal convictions and offences.

Large-scale public monitoring

This includes any personal data processing that occurs in a publicly accessible space.

The most prominent example of this is CCTV, but organisations will need to be increasingly concerned about the risks identified with dashcam footage and smart technology.

Likewise, the development of ‘smart cities’ will see a surge in public monitoring that will be subject to DPIAs.

In addition to these types of data processing, the ICO (Information Commissioner’s Office) states that organisations must conduct a DPIA when:

Implementing new technology

This includes processing that involves the innovative use of technologies or the application of modern technology to existing processes.

Examples of this include artificial intelligence and machine learning, self-driving cars and smart technology.

Automated decision-making

Organisations often use automated decision-making to decide whether an individual should be given access to a product or service.

You will often need to conduct a DPIA if these decisions involve the processing of personal data – but it will be particularly important if sensitive data is used.

For example, credit checks and mortgage applications use financial data, which poses an especially high risk if compromised, so a DPIA is essential.

Conducting large-scale processing

According to the ICO, all large-scale data processing – not just activities involving sensitive information – should be subject to a DPIA.

Processing biometric or genetic data

Biometric data is usually used to authenticate that someone has appropriate access rights. Face and iris recognition and fingerprint scans are the most common examples.

Physical tests, like heartbeat monitoring and keystroke dynamics, are also considered biometric data.

Similarly, the collection of genetic data (other than that processed by an individual GP or health professional for the provision of healthcare directly to the data subject) is subject to a DPIA.

This includes data processed to perform medical diagnoses, DNA testing or medical research.

Data matching

This is any activity in which personal data from multiple sources is combined or compared.

The software firm Data Ladder has compiled a detailed list of reasons why organisations might conduct data matching, with fraud prevention and direct marketing being two of the most common.

Conducting invisible processing

This is the processing of personal data that wasn't obtained directly from the data subject. The rules surrounding this are outlined in Article 14 of the GDPR

(<http://www.privacy-regulation.eu/en/article-14-information-to-be-provided-where-personal-data-have-not-been-obtained-from-the-data-subject-GDPR.htm>)

.

Examples of invisible processing include list brokering, direct marketing and online tracking by third parties.

Tracking

This is the monitoring of individuals' movement or behaviour. Depending on the organisation's aims, it might choose to track location, browsing history, health monitoring or interactions with IoT devices.

Targeting children or vulnerable people

Children and vulnerable people are given special protection under the GDPR.

This includes any personal data processing targeted at them for marketing purposes, profiling and other forms of automated decision-making.

Processing that involves risk of physical harm

The risk related to personal data breaches usually refers to financial, reputational or emotional damages. Still, you must also be aware of physical risks.

For example, if the identity of a whistle-blower was exposed, that person might fear for their safety.

Likewise, if child counselling records were exposed, the affected child's home life could be made even worse.

9. What is a Data Protection Officer?

Data Protection Officers (DPOs) are independent data protection experts who are responsible for:

- Monitoring an organisation's data protection compliance;
- Informing it of and advising on its data protection obligations;
- Providing advice on DPIAs (data protection impact assessments) and monitoring their performance; and
- Acting as a contact point for data subjects and the relevant supervisory authority – the ICO (Information Commissioner's Office) in the UK.

Under the EU GDPR (General Data Protection Regulation) (<https://gdpr-info.eu/>), many organisations are required to appoint a DPO to ensure compliance.

9.1. How to become a Data Protection Officer?

9.1.1. What do Data Protection Officers do?

A DPO is an independent data protection expert who is responsible for advising an organisation on how to comply with its regulatory requirements.

Their tasks include:

- Advising staff on their data protection responsibilities;
- Monitoring the organisation's data protection policies and procedures;
- Advising management on whether DPIAs (data protection impact assessments) are necessary;
- Serving as the point of contact between the organisation and its supervisory authority; and
- Serving as a point of contact for individuals on privacy matters.

A full list of the DPO's responsibilities are outlined in Article 39 of the GDPR.

9.1.2. What skills and experience are required?

DPOs must have a strong understanding of data protection law and regulatory requirements.

They also need good communication skills, as they'll be working with an organisation's staff and management, as well as with its supervisory authority.

Perhaps surprisingly, you don't need a formal qualification to become a DPO.

9.1.3. Can organisation's employee be a DPO?

Yes. The position can be filled internally or externally on either a full-time or part-time basis.

Be careful when appointing internally, though – particularly if the employee is maintaining their existing position.

The GDPR stipulates that a DPO must work independently and without instruction from their employer, as well as being free from any conflicts of interest.

An employer should not provide guidance on how to investigate complaints, what results should be achieved or how to interpret data protection law.

Similarly, DPOs can't have competing objectives, where business objectives could be prioritised over data protection.

There are circumstances in which an employee can take on the DPO's responsibilities alongside their own without a conflict of interest, but we suggest avoiding the risk.

Even if you are confident that there is no problem, job roles and responsibilities often evolve over time, and a conflict of interest might arise without you noticing.

9.1.4. Can organisations share a DPO?

Yes. It's an ideal alternative to assigning one of your own employees as DPO, allowing you to avoid the possibility of a conflict of interest while still not having to appoint a full-time, salaried DPO.

Whether you outsource the role or not, you must be careful about the DPO's requirements. Many organisations aren't legally required to appoint a DPO, but appoint someone to fill the role because it helps their overall GDPR compliance practices.

However, 'DPO' is a clearly defined job role, and if someone fills that position, they must fulfil the tasks that come with that.

If you want expert help but don't need a DPO specifically, it's advisable to consider them a 'GDPR Manager' or 'Data Privacy Officer'.

9.1.5. Steps to becoming a Data Protection Officer

The route to becoming a DPO depends on how much experience you have with the GDPR.

If you've already taken a GDPR Foundation training course, you can gain everything they need from a Certified Data Protection Officer (C-DPO) Training Course.

Meanwhile, if you've completed the GDPR Foundation and Practitioner training courses, you only need to take the Certified Data Protection Officer (C-DPO) Accelerated Training Course.

DPOs with two years' experience can skip the training step and simply sit the exam.

If the exam is passed, the DPO will be certified by IT Governance for two years, with the option of renewing their certification after that. The DPO must demonstrate at least one year of further DPO experience to be able to recertify.

10. GDPR's requirements for an EU representative

The run-up to Brexit has seen increased discussion in the UK about the need for an EU representative under the GDPR (General Data Protection Regulation).

Organisations must appoint an EU representative if they are based outside the EU and monitor the behaviour of, or provide goods or services to, EU residents.

This requirement fell under the radar at the time the GDPR took effect, because it would only apply in the UK after Brexit.

Already swamped with compliance requirements, organisations focused on their immediate priorities and left their EU representative requirements until a later date.

That date has now come. The UK is set to leave the EU at the end of 2020 and, as soon as it does, organisations based in the country are legally required to have an EU representative.

10.1. What does an EU representative do?

As the title suggests, EU representatives must be established in the EU and work on behalf of non-EU-based organisations.

In the case of UK organisations, this will primarily involve serving as the point of contact between the organisation, the ICO (Information Commissioner's Office) and data subjects.

They'll do this by:

- Responding to any queries the ICO or data subjects have concerning data processing;
- Maintaining records of the organisation's data processing activities; and
- Making data processing records accessible to the ICO.

10.2. What's the difference between an EU representative and a DPO?

The tasks of an EU representative sound a lot like those of a DPO (Data Protection Officer), but don't confuse the two.

An EU representative is tasked with representing non-EU based organisations when it comes to their GDPR requirements. In other words, they are a function of the organisation's GDPR compliance

practices.

By contrast, a DPO is an independent expert who helps facilitate and assess the organisation's compliance practices. They are responsible for monitoring compliance and advising organisations on how to navigate their requirements.

10.3. Do all UK organisations need an EU representative?

UK organisations only need to appoint an EU representative if they monitor or provide goods or services to EU residents.

If you deal exclusively with UK-based customers, you won't be required to appoint an EU representative. That's because as soon as the UK is no longer in the EU, your customers will cease to be EU residents.

However, if your data processing or monitoring extends to other EU member states, you'll probably be required to appoint an EU representative. There are two exemptions:

- Organisations that have an office and employees based in the EU.
- Organisations whose processing activity is occasional, doesn't include large-scale processing of special categories of data and is unlikely to result in a risk to the rights and freedoms of natural persons (see Article 27 of the GDPR for more information).

10.4. Selecting your EU representative

Your EU representative can be any natural or legal person who's based in an EU member state within which you collect personal data.

If you only collect information from data subjects in, say, France, your EU representative must be based in France. However, if you collect personal data from the entirety of the EU, you can appoint a representative in any EU member state.

When you have multiple countries to choose from, it's best to select the one in which you collect the most data or conduct the most extensive monitoring.

11. Do I need a lot of documents to comply with the GDPR?

The GDPR's accountability principle requires you to complete dozens of documents to prove that you have the necessary policies and procedures in place, includes:

- Data protection policy
- Training policy
- Information security policy
- Data protection impact assessment procedure
- Retention of records procedure
- Data subject access request form and procedure
- Privacy procedure
- Privacy notice
- International data transfer procedure
- Data portability procedure
- Audit checklist

11.1. List of mandatory documents required by the GDPR

The documentation of processing activities is a new legal requirement under the EU GDPR (General Data Protection Regulation) (<https://gdpr-info.eu/>).

Documenting your processing activities can also support good data governance, and help you to demonstrate your compliance with other aspects of the GDPR.

In this post we have listed all of the documentation, policies and procedures you must have if you want to be fully GDPR compliant.

11.1.1. Mandatory documents for GDPR compliance

Personal Data Protection Policy (Article 24)

A data protection policy is a statement that sets out how your organisation protects personal data.

It explains the GDPR's requirements to your employees, and demonstrates your organisation's commitment to compliance.

Privacy Notice (Articles 12, 13, and 14)

A privacy notice is a public statement of how your organisation applies (and complies with) the GDPR's data processing principles.

An essential part of compliance, it serves two purposes: to promote transparency, and to provide individuals with more control over the way their data is used.

Employee Privacy Notice (Articles 12, 13 and 14)

Under the GDPR, you must be more transparent and open than ever before about the employee-related data you process.

It is also a core GDPR principle for employers to process HR related data in a fair and transparent way.

An employee privacy notice is a key step towards compliance, and explains to an individual how a data controller (in this case, your organisation) processes an employee's personal data.

Data Retention Policy (Articles 5, 13, 17, and 30)

A data retention (or records retention) policy outlines your organisation's protocol for retaining information.

It is important that your organisation only retains data for as long as it's needed.

This is because holding on to data for longer than necessary can take up valuable storage space and incur unnecessary costs.

When writing your data retention policy, you should consider two key factors:

- How you are going to organise information so it can be accessed at a later date; and
- How you will dispose of information that is no longer needed.

Data Retention Schedule (Article 30)

A data retention (or records retention) schedule is a policy that defines how long data items must be kept.

It also provides disposal guidelines for how data items should be discarded.

Data Subject Consent Form (Articles 6, 7, and 9)

Consent is one lawful basis for processing personal data, and explicit consent can also legitimise the use of special category data.

If your organisation is processing personal data for a specific purpose, you must obtain permission from the data subjects in question with a consent form.

Consent under the GDPR is often misunderstood and mismanaged.

Below, a best-practice guidance for writing a GDPR consent form.

WRITING A GDPR CONSENT FORM

BEST-PRACTICE GUIDANCE

Request as little data as possible

Data should be collected for a specific purpose, used only for that purpose and retained for only as long as it meets that purpose.

Make the terms and conditions clear

Consent mechanisms must be easy to use and kept separate from other terms and conditions, and requests must be written clearly and concisely.

Make it easy to withdraw consent

Individuals need to be told straight away that they can withdraw their consent at any time, and you must explain how to do it.

Supplier Data Processing Agreement (Articles 28, 32, and 82)

If you use another organisation (i.e. a sub-processor) to assist with your processing of personal data, you need to have a written contract in place with that sub-processor.

This is known as a supplier data processing agreement.

DPIA Register (Article 35)

The DPIA Register is used to document your organisation's Data Protection Impact Analysis (DPIA).

Data Breach Response and Notification Procedure (Articles 4, 33, and 34)

You must create a procedure that applies in the event of a personal data breach under Article 33 –

“Notification of a personal data breach to the supervisory authority” – and Article 34 of the GDPR – “Communication of a personal data breach to the data subject”.

Below is an example of what a data breach notification might look like:

PERSONAL DATA BREACH
NOTIFICATION PROCEDURE (TIER 2)

Document Control

Reference: GDPR.DOC.2.5

Issue No:

Issue Date:

Page: 1 of 4

IT Governance are experienced data protection practitioners and all document templates are provided as general guidance. Users of these documents should consult their own legal advisers for legal advice specific to their own circumstances and IT Governance accepts no liability of any sort arising from the use of these templates.

1. Scope

This procedure applies in the event of a personal data breach under Article 33 of the GDPR – Notification of a personal data breach to the supervisory authority – and Article 34 – Communication of a personal data breach to the data subject.

The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Each organisation should establish whether it is data controller, or a data processor for the same data processing activity; or whether it is a joint controller.

2. Responsibility

2.1 All users (whether Employees/Staff, contractors or temporary Employees/Staff and third party users) and [owners] of Organisation Name are required to be aware of, and to follow this procedure in the event of a personal data breach (reference Training Policy [GDPR.DOC.1.1](#)).

2.2 All Employees/Staff, contractors or temporary personnel are responsible for reporting any personal data breach to the Data Protection Officer/ Head of IT (CIO).

3. Procedure – Breach notification data processor to data controller

3.1 Organisation Name reports any personal data breach or security incident to the data controller without undue delay [if you process data for a number of controllers, where is this information specified?]. These contact details are recorded in the Internal Breach Register ([GDPR.REC.4.5](#)). Organisation Name provides the controller with all of the details of the breach.

3.2 The breach notification is made by [email, phone call, etc.].

3.3 A confirmation of receipt of this information is made by [email, phone call, etc.].

4. Procedure – Breach notification data controller to supervisory authority

Author

The [Data Protection Officer (DPO)] has a specific task under article 39 of the GDPR to coordinate with the supervisory authority and act as the focal point for matters pertaining to processing.

Author

If your organisation is solely a data controller, this won't apply.

Author

The data processing contract between the controller and the processor should have all the contact details and relevant procedures for making contact regarding data breaches.

Author

Best practice would be to record this in two forms of communication (for example, email and phone call).

Author

The data controller needs all details before deciding how to proceed.

Organisation Name

Classification_3

Insert

Customisable PROCEDURE template v2.0

Data Breach Register (Article 33)

You must maintain an internal record of all personal data breaches in a Data Breach Register.

The data breach register should contain details of the facts surrounding the breach, the effects of the breach, and any remedial action taken.

Data Breach Notification Form to the Supervisory Authority (Article 33)

If you have experienced a personal data breach that needs to be reported to the ICO, you will need to fill in the applicable data breach notification form.

For more information on data breach reporting, [visit the ICO’s website](#)

(<https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>).

Data Breach Notification Form to Data Subjects (Article 34)

You will need to complete a Data Breach Notification Form to Data Subjects if you have experienced a personal data breach that is likely to result in a “high risk to the rights and freedoms” of an individual.

GDPR documentation only required under certain conditions

11.1.2. Documents only required under certain conditions

Some GDPR documents are only applicable under certain conditions, including:

Data Protection Officer Job Description (Articles 37, 38, and 39)

You’ll need to appoint a DPO if:

- You are a public authority or body, except for courts acting in their judicial capacity; or
- Your core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or
- Your core activities process on a large scale special categories of data and personal data relating to criminal convictions and offences.

Inventory of Processing Activities (Article 30)

This document is mandatory if:

- Your organisation has more than 250 employees; or
- The processing the you carry out is likely to result in a risk to the rights and freedoms of data subjects; or
- The processing is not occasional; or
- The processing includes special categories of data; or
- The processing includes personal data relating to criminal convictions and offences.

Standard Contractual Clauses for the Transfer of Personal Data to Controllers (Article 46)

This document is mandatory if you are transferring personal data to a controller outside the European Economic Area (EEA) and you are relying on model clauses as your lawful grounds for cross-border data transfers.

Standard Contractual Clauses for the Transfer of Personal Data to Processors (Article 46)

This document is mandatory if you are transferring personal data to a processor outside the European Economic Area (EEA) and you are relying on model clauses as your lawful grounds for cross-border data transfers.

12. How to write a GDPR Data Privacy Notice?

Under the GDPR (General Data Protection Regulation) (<https://gdpr-info.eu/>), organisations must provide individuals with certain information via a data privacy statement or privacy notice.

But what is a data privacy notice, and what should it contain?

12.1. What is a privacy notice?

A privacy notice is one of several documents required for GDPR compliance.

But whereas many of these documents are strictly internal, a privacy notice is provided to customers and other interested parties, explaining how the organisation processes their personal data.

There are two reasons for doing this. First, it prevents any confusion about the way personal data is being used and ensures a level of trust between the organisation and the individual.

Second, it gives individuals more control when an organisation collects their personal data. If there's something they aren't happy with, they can query it via a DSAR (data subject access request) and ask the organisation to suspend that processing activity.

12.2. How to write a privacy notice

Article 30 of the GDPR explains that a compliant document should include the following details:

12.2.1. Contact details

The first thing to include in your privacy notice is the name, address, email address and telephone number of your organisation.

If you've appointed a DPO (Data Protection Officer) or EU representative, you should also include their contact details.

12.2.2. The types of personal data you process

The definition of personal data is a lot broader than you might think, so you must ensure you've included everything necessary – and in specific detail.

For example, instead of just saying 'financial information', state whether it's account numbers, credit card numbers, etc.

You should also outline where you obtained the information if it wasn't provided by the data subject

directly.

12.2.3. Lawful basis for processing personal data

Under the GDPR, organisations can only process personal data if there is a lawful basis for doing so. Your privacy policy should specify which one you're relying on for each processing purpose.

If you are relying on legitimate interests, you must describe them. Likewise, if you're relying on consent, you should state that it can be withdrawn at any time.

Remember that there are specific rules when it comes to processing special categories of personal data.

12.2.4. How you process personal data

You must explain whether you will be transferring personal data to third parties.

We suggest also specifying how you will protect shared data, particularly when the third party is based outside the EU.

12.2.5. How long you'll be keeping their data

The GDPR states that you can only retain personal data for as long as the legal basis for processing is applicable.

In most cases, that will be easy to determine. For example, data processed to fulfil contracts should be stored for as long as the organisation performs the task to which the contract applies.

Likewise, organisations should hold on to any data processed on the grounds of a legal obligation, public task or vital interest for as long as those activities are relevant.

Things are trickier with consent and legitimate interests, as there is no clear point at which they're no longer valid.

As such, we recommend reviewing your data retention practices at least every two years.

12.2.6. Data subject rights

The GDPR gives individuals eight data subject rights, which you should list and explain in your privacy notice:

- Right to be informed: organisations must tell individuals what data of theirs is being collected, how it's being used, how long it will be kept and whether it will be shared with any third parties.

- Right of access: individuals have the right to request a copy of the information that an organisation holds on them.
- Right of rectification: individuals have the right to correct data that is inaccurate or incomplete.
- Right to be forgotten: in certain circumstances, individuals can ask organisations to erase any personal data that is stored on them.
- Right of portability: individuals can request that an organisation transfers any data that it holds on them to another company.
- Right to restrict processing: individuals can request that an organisation limits the way it uses personal data.
- Right to object: individuals have the right to challenge certain types of processing, such as direct marketing.
- Rights related to automated decision making, including profiling: individuals can ask organisations to provide a copy of its automated processing activities if they believe the data is being processed unlawfully. You should also remind individuals that they are free to exercise their rights and explain how they can do this.

13. How do you write a GDPR DSAR (Data Subject Access Request) procedure?

13.1. What is a data subject access request?

Article 15 states that data controllers must confirm to data subjects whether their personal data is being processed, and, where it is, provide them with a copy of that personal data (providing it does not adversely affect the rights and freedoms of others).

They must also state:

- The purposes of the processing;
- The categories of personal data involved;
- The recipients (or categories of recipients) to whom the personal data has been or will be disclosed;
- The envisaged period for which the personal data will be stored (or, if this is not possible, the criteria used to determine that period);
- The existence of the right to request that the controller rectify or erase the personal data or restrict processing, or to object to processing;
- The right to lodge a complaint with a supervisory authority;
- Where the personal data has not been collected direct from the data subject, any available information about its source; and
- The existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences for the data subject of such processing.

It's therefore essential to establish a procedure for responding to DSARs.

13.2. Data subject access request procedures under the GDPR

Your DSAR procedure should ensure you are able to meet the following requirements:

- In most circumstances, the information requested must be provided free of charge.
- Organisations are permitted to charge a “reasonable fee” when a request is manifestly unfounded, excessive or repetitive. This fee must be based on the administrative cost of providing the information.

- Information must be provided without delay and within a month.
- Where requests are complex or numerous, organisations are permitted to extend the deadline to three months. However, they must still respond to the request within a month to explain why the extension is necessary.
- Data subjects must be able to make requests electronically as well as physically, “especially where personal data are processed by electronic means”.
- DSARs can be made in any form, including through email, phone call or web contact forms.

And Recital 63 recommends that, where possible, “the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data”.

13.3. What is included in a data subject access request?

A request might refer to specific personal details or processes for which the organisation processes that information, in which case you only need to provide relevant information.

However, individuals may ask to see a full list of the personal data that the organisation stores on them.

This will undoubtedly be burdensome, because it’s not merely a case of pulling up everything you store on that person.

If you did that, you’d end up with large volumes of information that aren’t considered personal data – such as internal memos about the data subject’s files – which don’t need to be shared.

Your first tasks, therefore, are to determine what information related to the individual is considered personal data under the definition of the GDPR, and whether it’s part of the data that they requested.

This information must be provided alongside other supplementary material, such as the relevant details provided in the organisation’s privacy notice.

13.4. Can information be redacted?

Although the GDPR promotes openness to the public, organisations can and, where relevant, should redact anything that’s not within the scope of the DSAR.

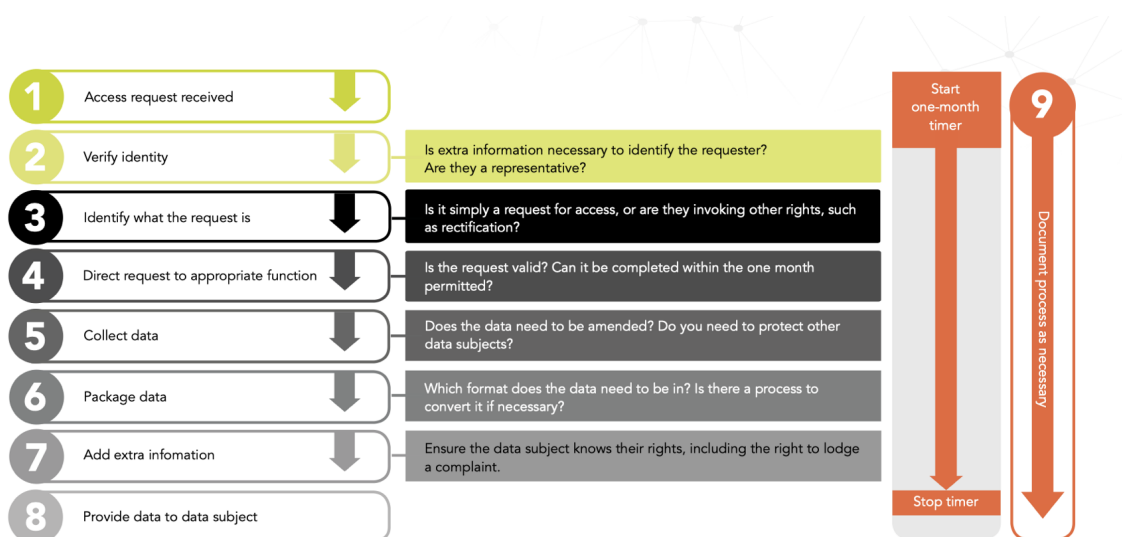
For example, you might have documents that include that individual’s personal data alongside the personal details of other people.

In these circumstances, you are required to redact all personal data that isn't about the person making the request, because otherwise, you'd be committing a data breach.

Likewise, you might have records where the individual's personal data is stored alongside sensitive company data. You are within your rights to redact that information.

13.5. Infographic: data subject access request flowchart

Are you following the correct steps when responding to a data subject access request?



13.6. Do individuals have to give a reason for a DSAR?

Individuals don't need to state why they are submitting a DSAR. The only questions an organisation may ask when a DSAR is submitted concern verifying the individual's identity or to help them locate the requested information.

13.7. Does a request have to be in writing?

There is no formal process for submitting a DSAR. That means requests don't need to be submitted in writing – or in any documented way. For example, an individual can make a request while speaking with a member of staff.

It's also worth noting that individuals aren't required to use the technical term for a request ('DSAR' or 'data subject access request').

They can, for instance, simply say that they'd like to see a copy of the information the organisation

stores on them.

That said, requests are most likely to be submitted in writing, as it's the most convenient method.

It gives individuals and organisations a record of the request, the date that it was made and other relevant information, such as the specific personal information that they want a copy of and the format that it should be delivered via.

13.8. Can individuals submit a DSAR on behalf of someone else?

Yes, individuals can authorise someone else to make a request on their behalf. This is most likely to happen when:

- Someone with parental responsibility asks for information about a child;
- A court-appointed individual is managing someone else's affairs;
- A solicitor is acting on their client's instructions; and
- The data subject requests help from a relative or friend.

Organisations must, of course, be satisfied that the person making the request really is doing so on behalf of the data subject.

As such, they are entitled to request supporting evidence, such as written authorisation from the data subject or a more general power of attorney.

13.9. How long do organisations have to respond to a DSAR?

There is a subject access request time limit. DSARs must be fulfilled "without undue delay", and at the latest within one month of receipt.

Where requests are complex or numerous, organisations are permitted to extend the deadline to three months. However, they must still respond to the request within a month and explain why the extension is necessary.

13.10. Who is responsible for responding to a subject access request?

An organisation's Data Protection Officer (DPO) will generally be responsible for fulfilling a DSAR, provided the organisation has appointed one.

If you don't have a DPO, the duty should fall to someone in your workforce with data protection knowledge.

In either case, the expert probably won't do the physical work involved in completing the request, such as combing through documents and redacting information.

Still, they will oversee the process and ensure that it is being completed in line with the GDPR's requirements.

13.11. How much can be charged for a subject access request?

Under the GDPR's predecessor, the DPA (Data Protection Act) 1998, organisations could charge a fee for fulfilling a DSAR, but that's no longer the case in most instances.

Indeed, as the UK's data protection supervisory authority, the ICO (Information Commissioner's Office), explains, there are only two instances when organisations may now only request payment for a DSAR.

These are when a request is manifestly unfounded (i.e. when the individual clearly has no intent to exercise their right of access, such as when the request is an excuse to make unsubstantiated accusations against the organisation) or excessive (i.e. when the request overlaps with a recently submitted DSAR).

Organisations should base the fee they charge on the administrative costs involved. That's to say; they shouldn't be profiting from requests.

It's worth adding that organisations are within their rights to reject manifestly unfounded or excessive requests outright instead of charging a fee for them. This might be the case when they simply don't have the time or resources to fulfil the request.

13.12. What's the difference between a freedom of information request and a DSAR?

DSARs might sound a lot like freedom of information (FOI) requests, but in practice, they are a lot different.

Whereas DSARs grant EU residents access to copies of their personal data, FOI requests are specific to the UK and relate to recorded information held in the public sector.

This generally refers to government departments, local councils and regulators, such as the Financial

Conduct Authority.

Additionally, personal data is not covered by the FOI Act, so there are no restrictions on who can make a request.

13.13. The process for handling a DSAR

Like many aspects of the GDPR, access requests have a formal name that organisations must be aware of for compliance purposes, but that doesn't mean individuals need to know the terminology.

As the ICO (Information Commissioner's Office), the UK's data protection supervisory authority, notes, there's no specific process for making a request, so someone could simply say "I'd like to see what data you have on me", and that would be considered a legitimate request.

As such, it's essential that anyone in your organisation who may receive such a request knows what to look out for and who to pass the message on to.

In many organisations, the DPO will be responsible for handling DSARs. However, if you aren't required to appoint one, you'll need to find an alternative approach.

Since time is of the essence when responding to a DSAR, it's a good idea to ensure you have an established DSAR process beforehand, so that you can deal with such requests quickly.

13.13.1. Verify the identity

One of the first steps is to verify the identity of the requester so that you can determine whether you have all the information you need to fulfil the request.

13.13.2. Clarify what the request is

Following that, find out a bit more about the request itself. Is it merely a request for access, or are they invoking other rights, such as rectification of the personal data being held?

13.13.3. Is the request valid?

Establish whether the request is valid and if it can be completed within the one-month period. If not, you can take further steps to request an extension.

13.13.4. Inspect the data

Once you start collecting the data, check whether the data needs to be amended and if you need to protect the personal information of any other data subjects.

13.13.5. Choose the format

Once you've collected all the data, determine the most appropriate format in which to provide the information.

13.13.6. Add extra information

Lastly, before sending the information, ensure the data subjects know their rights, including the right to lodge a complaint.

13.14. How to ensure data subject access request success

There are many steps you can take to help your organisation manage DSARs. Your first task is to create a flowchart to make sure you respond promptly, thoroughly and in line with the GDPR's requirements.

There are also ways you can make your organisation more resilient to the challenges that come with responding to DSARs. For example, you should implement measures addressing:

13.14.1. Staff training

Data subjects can theoretically submit a DSAR whenever they're communicating with a member of your staff. You must, therefore, make sure that all relevant employees can recognise a request and know how to respond.

13.14.2. DSAR responsibilities

You should appoint someone or a team of people to take responsibility for responding to DSARs. This might be your DPO, or it could be another employee who is familiar with the GDPR's compliance requirements.

If only one person takes on this task, you must make sure other employees know how to complete a request so that they can fill in during holidays or other absences.

13.14.3. Expert advice

Unless you were able to appoint an experienced DPO to oversee access requests, there's a good chance that the person overseeing your response process is relatively new to the task.

In most cases that won't be a problem, because once you get into the swing of things, it's a relatively routine operation. However, there will be some challenging requests that require guidance, such as through one-off consultancy services.

14. How to Write a GDPR Data Protection Policy?

The GDPR (General Data Protection Regulation) (<https://gdpr-info.eu/>) isn't just about implementing technological and organisational measures to protect the information you store.

You also need to demonstrate your compliance, which is why data security policies are essential.

These documents form part of organisations' broader commitment to accountability, outlined in Article 5(2) of the GDPR

(<https://www.privacy-regulation.eu/en/article-5-principles-relating-to-processing-of-personal-data-GDPR.htm>).

14.1. What is a data protection policy?

A data protection policy is an internal document that serves as the core of an organisation's GDPR compliance practices.

It explains the GDPR's requirements to employees, and states the organisation's commitment to compliance.

The data protection policy doesn't need to provide specific details on how the organisation will meet the Regulation's data protection principles, as these will be covered in the organisation's procedures.

Instead, a policy only needs to outline how the GDPR relates to the organisation. Take data minimisation as an example.

Whereas your procedures should state exactly how you will ensure this principle will be met (for example, you might require that any prospective data collection activities be accompanied by a document explaining why processing is necessary), your policy need only state that the organisation will address that principle.

14.2. Why do you need a GDPR data protection policy?

Data protection policies serve three goals. First, they provide the groundwork from which an organisation can achieve GDPR compliance.

The Regulation as it's written is too complex to be used as a basis for an implementation project. Imagine starting on page one and planning your compliance practices as you go; it would be a mess.

Instead, you should use the policy as a cheat sheet, breaking the GDPR's requirements into manageable chunks that apply to your organisation.

That brings us to the second goal: to make the GDPR understandable to your staff. Remember, most employees who handle personal data aren't data experts and won't have pored over the Regulation's principles to understand why these rules are in place.

A data protection policy is the ideal place to address that, explaining in simple terms how the GDPR applies to them and what their obligations are.

Finally, data protection policies prove that organisations are committed to preventing data protection breaches.

Article 24 of the GDPR

(<http://www.privacy-regulation.eu/en/article-24-responsibility-of-the-controller-GDPR.htm>) specifies that organisations create a policy in order to “demonstrate that [data] processing is performed in accordance with this Regulation”.

Being able to demonstrate compliance is essential when it comes to regulatory investigations.

If a customer complains that an organisation has misused their data or hasn't facilitated one or more of their rights as a data subject, the organisation will be subject to an investigation from their supervisory authority.

A data protection policy will be the first piece of evidence the regulator looks for to see whether the organisation takes the GDPR seriously.

From there, the supervisory authority may determine whether the organisation processes personal data lawfully, and if it didn't, whether the violation was due to a mistake or widespread neglect of the Regulation's requirements.

The answer to this will determine what disciplinary action is levied. A one-time mistake might be met with a slap on the wrist and a reminder to be more thorough in the future, but a systemic failure will almost certainly lead to a significant fine.

The UK GDPR and DPA 2018 set a maximum fine of £17.5 million or 4% of annual global turnover – whichever is greater – for infringements.

The EU GDPR sets a maximum fine of €20 million (about £18 million) or 4% of annual global turnover – whichever is greater – for infringements.

14.3. What your data protection policy should include

You can include as much or as little information in your GDPR data protection policy as you like, but we recommend that you cover:

- **The purpose of the policy:** This can serve as your introduction, explaining the policy's relation to the GDPR, the importance of compliance and why the policy is necessary.
- **Definition of key terms:** The GDPR is full of data protection terminology that you will need to explain. This section should include notoriously tricky terms like 'data controller' and 'data processor', but you might also want to clarify things like 'data subject', which aren't as clear-cut as you might think.
- **Scope:** The GDPR's requirements apply to EU residents' personal information and anyone in your organisation who processes that data. You must also define what types of information the GDPR applies to. Part of the reason for doing this is that the Regulation distinguishes 'special categories of personal data', which are subject to extra protection.
- **Principles:** Explain the GDPR's six principles for data processing, as well as accountability (which is also a principle but addressed slightly differently). You should also briefly note your commitment to meeting these principles.
- **Data subject rights:** The GDPR endows individuals with eight data subject rights. You should define them and state that will ensure that they are met.
- **DPO (Data Protection Officer):** You should provide the name and contact details of your DPO. If you've chosen not to appoint one (some organisations are exempt from this requirement), you should list the senior member of staff responsible for data protection.

15. How to write a GDPR data retention policy?

Under the General Data Protection Regulation (GDPR), organisations must create a data retention policy to help them manage the way they handle personal information.

If you keep sensitive data for too long – even if it’s being held securely and not being misused – you may still be violating the Regulation’s requirements.

That might sound overly strict, but there’s a good reason for it.

15.1. What is a data retention policy?

A data retention policy is a set of guidelines that helps organisations keep track of how long information must be kept and how to dispose of the information when it’s no longer needed.

The policy should also outline the purpose for processing the personal data. This ensures that you have documented proof that justifies your data retention and disposal periods.

15.2. Aims and objectives

If you cast your mind back to the panic that preceded the GDPR taking effect, you’ll have a perfectly good understanding of why data retention periods are essential.

Organisations that hadn’t interacted with us in years came out of the woodwork to ask for our consent to keep hold of our data.

It showed just how often our records sit on organisation’s databases long after we’ve finished using their services.

The organisation doesn’t want to get rid of the information, because it costs practically nothing to store customer details, but keeping it unnecessarily exposes it to security threats.

It only takes one piece of bad luck for an organisation’s systems to be breached, whether it’s a cyber attack or an internal error.

So, to limit the damage that data breaches can cause, regulators mandated that EU-based organisations must retain personal data only if there’s a legitimate reason for keeping it.

15.3. How long can personal data be stored?

Despite the apparent strictness of the GDPR's data retention periods, there are no rules on storage limitation.

Organisations can instead set their own deadlines based on whatever grounds they see fit. The only requirement is that the organisation must document and justify why it has set the timeframe it has.

The decision should be based on two key factors: the purpose for processing the data, and any regulatory or legal requirements for retaining it.

Data should not be held for longer than is needed and shouldn't be kept 'just in case' you have a need for it in the future.

As long as one of your purposes still applies, you can continue to store the data.

You should also consider your legal and regulatory requirements to retain data. For example, when the data is subject to tax and audits, or to comply with defined standards, there will be data retention guidelines you must follow.

You can plan how your data will be used and if it will be needed for future use by creating a data flow map. This process is also helpful when it comes to locating data and removing it once your retention period expires.

There are two ways you can avoid data retention deadlines. The first is by anonymising data; this means that the information cannot be connected to an identifiable data subject.

If your data is anonymised, the GDPR allows you to keep it for as long as you want.

You should be careful when doing this, however. If the information can be used alongside other information the organisation holds to identify an individual, then it is not adequately anonymised.

You can also circumvent data retention deadlines if the information is being kept for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

15.4. What to do with data past the retention period

You have two options when the deadline for data retention expires: delete it or anonymise it.

If you opt to delete the data, you must ensure all copies have been discarded. To do this, you will need to find out where the data is stored. Is it a digital file, hard copy or both?

It's easy to erase hard copy data, but digital data often leaves a trace and copies may reside in forgotten file servers and databases.

To comply with the GDPR, you will need to put the data 'beyond use'. All copies of the data should be removed from live and back-up systems.

15.5. How to create a data retention policy

Your data retention policy should be part of your overall information security documentation process.

The first step is to gain a full picture of exactly what data you're processing, what it's being used for and which regulations apply to your business.

These regulations include, but aren't necessarily limited to, the GDPR. For example, if you process individuals' debit or credit card information, you may be subject to the PCI DSS (Payment Card Industry Data Security Standard).

Similarly, if you intend to comply with ISO 27001, the international standard that describes best practice for information security, you must take note of its requirements.

These compliance requirements will dictate what information must be included in your policy and the rules it should follow.

A simple data retention policy will address:

- The types of information covered in the policy: Different types of information will be subject to different rules, so you must keep a record of what data you are processing – whether that's names, addresses, contact details, financial records and so on.
- How long you are entitled to keep information: Clients are sometimes surprised when we tell them that GDPR does not set out specific time limits for data to be held. The length of time you hold particular data for is a subjective decision for you to make based on your reasons for processing the data.
- What you should do with data when it's no longer needed: Regular deletion of unnecessary data also reduces the amount of data you need to sift through to comply with subject access requests. It also reduces the costs of storage and document management.

Going through your data retention policy regularly allows you to clean house and remove duplicated and outdated files to avoid confusion and expedite any necessary searches.

16. How do you write a GDPR PRBN (Personal Data Breach Notification) procedure?

Articles 33 and 34 set out the conditions for notifying the supervisory authority of data breaches and communicating breaches to data subjects.

They state that:

- Data processors must report all breaches of personal data to data controllers “without undue delay”;
- Data controllers must report breaches to the supervisory authority (the ICO in the UK) within 72 hours of becoming aware of them if there is a risk to data subjects’ rights and freedoms; and
- Data subjects themselves must be notified “without undue delay” if there is a high risk to their rights and freedoms.

16.1. What is a personal data breach?

The ICO (Information Commissioner’s Office) defines a personal data breach as any event that results in “the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data”.

This includes incidents that involve:

- Unauthorised access from a third party;
- Deliberate or accidental action (or inaction) by a data controller or data processor;
- Sending personal data to an unintended recipient;
- Lost or stolen computing devices containing personal data;
- Unauthorised alteration of personal data; and
- Loss of availability of personal data.

16.2. Personal data breach notification procedures under the GDPR

Organisations must create a procedure that helps them respond in the event of a personal data breach.

This requirements for this are outlined in Article 33 and Article 34 of the GDPR.

17. GDPR Article 30: How do you comply with?

The principle of accountability is an essential part of the GDPR. Organisations must not only comply with the Regulation but also be able to demonstrate that they comply. This requires thorough record-keeping. Article 30 sets out the data processing records that you must maintain.

These include:

- Your organisation's name and contact details;
- The purposes of the processing;
- Descriptions of the categories of data subjects and categories of personal data;
- The categories of recipients of personal data;
- Details of transfers to third countries and international organisations, if applicable;
- Envisaged data retention schedules for different categories of data, where possible; and
- A description of the technical and organisational security measures you have implemented.

A data map will help you identify the information your organisation processes, and exactly how it is processed.

17.1. Data mapping under the EU GDPR

To comply with the EU GDPR (General Data Protection Regulation) (<https://gdpr-info.eu/>), organisations need to map their data flows to assess privacy risks.

Conducting a data flow map forms part of your Article 30 documentation. They are also an essential first step in completing a DPIA (data protection impact assessment).

17.2. Creating data flow maps

17.2.1. Understand the information flow

Information flow is the transfer of information from one location to another, for example:

- From inside to outside the European Union; or
- From suppliers and sub-suppliers through to customers.

17.2.2. Describe the information flow

- Walk through the information lifecycle to identify unforeseen or unintended uses of data. This also helps to minimise what data is collected.
- Make sure the people who will be using the information are consulted on the practical implications.
- Consider the potential future uses of the information collected, even if it is not immediately necessary.

17.2.3. Identify its key elements

- Data items: What kind of data is being processed and what category does it fall into?
- Formats: In what format do you store data (hard copy, digital, database, bring your own device, mobile phones, etc.)?
- Transfer method: How do you collect data and how do you share it, both internally and externally?
- Location: What locations are involved within the data flow (offices, the Cloud, third parties, etc.)?
- Accountability: Who is accountable for the personal data? Often this changes as the data moves throughout the organisation.
- Access: Who has access to the data in question?
- Lawful basis: Identify the lawful basis used for processing the personal data.

17.3. The key challenges of data mapping

17.3.1. Identifying personal data

Personal data can reside in multiple locations and can be stored in many formats, such as paper, electronic and audio. Your first challenge is deciding what information you need to record and in what format.

17.3.2. Identifying appropriate technical and organisational safeguards

You need to protect information and determine who controls access to it. To do this, you will need to identify the appropriate technology and the policy and procedures for its use

17.3.3. Understanding legal and regulatory obligations

Your legal and regularity obligations may extend beyond the GDPR. This can include other compliance standards, such as the PCI DSS (Payment Card Industry Data Security Standard) and ISO 27001.

What is the PCI DSS?

The PCI DSS (Payment Card Industry Data Security Standard) is an information security standard

designed to reduce payment card fraud by increasing security controls around cardholder data.

The Standard results from a collaboration between the major payment brands (American Express, Discover, JCB, Mastercard and Visa), and is administered by the PCI SSC (Payment Card Industry Security Standards Council).

[Read the full text of PCI DSS v3.2.1 on the PCI Security Standards Council website.](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1574851396486)

(https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1574851396486)

ISO 27001 definition: What is ISO 27001?

ISO/IEC 27001:2013 (also known as ISO27001) is the international standard for information security. It sets out the specification for an information security management system (ISMS).

The information security management system standard's best-practice approach helps organisations manage their information security by addressing people, processes and technology.

Certification to the ISO 27001 Standard is recognised worldwide as an indication that your ISMS is aligned with information security best practice.

Part of the ISO 27000 series of information security standards, ISO 27001 is a framework that helps organisations “establish, implement, operate, monitor, review, maintain and continually improve an ISMS”.

The latest version of the ISO 27001 information security standard was published in September 2013, replacing the 2005 iteration.

18. GDPR Article 32: Guide to the requirements

Perhaps the most widely discussed set of compliance requirements within the GDPR (General Data Protection Regulation) are those found in Article 32.

That's because it contains the measures that organisations must implement to prevent cyber attacks and data breaches.

18.1. What is Article 32 of the GDPR?

Article 32 of the GDPR (<https://www.privacy-regulation.eu/en/article-32-security-of-processing-GDPR.htm>) sets out the technical and organisational measures that organisations should implement to protect the personal data that they store.

The Regulation doesn't go into specific detail about what these processes should look like, because best practices – particularly when it comes to technology – change rapidly and what is considered appropriate now might not be in a few years.

However, what is absolute is that any measures you implement should focus on the 'security of processing', which is Article 32's sub-header.

That means looking at the ways you store and protect personal data, and particularly at preventing data breaches as well as physical or technical incidents.

There are many other factors that go into GDPR compliance – such as your level of transparency with data subjects and your purpose(s) for processing their information – but these concerns can all be put aside for the moment.

To comply with Article 32, you need to identify and mitigate risks that are presented by data processing, "in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed".

So how can you do that? Let's take a look.

18.2. Minimum compliance requirements in Article 32

Every organisation operates uniquely and has its own risks, so there is no single set of data protection practices that work for everyone.

That's why the GDPR requires you to implement defences that are appropriate to your circumstances

and the risks that you face.

This could include:

18.2.1. Pseudonymising personal data

You can do this by replacing the names and unique identifiers of data subjects with a reference number, which you can cross-reference via a separate document. This way, the information poses much less risk if it is exposed.

This is a relatively simple approach to data security, and it's important to remember that it only helps to some extent. Indeed, should someone hack into your systems, they may be able to find the corresponding data set and identify the data subjects.

As such, some organisations might go the extra mile and encrypt personal data.

As with pseudonymisation, encrypted data is unreadable unless you have another piece of information – which, in this case, is a decryption key.

However, the extra security makes it more inconvenient to access the data, so you probably wouldn't encrypt a database that you were using regularly.

This process is much better suited to archives, files that you only occasionally access, data that's being transferred or information that's stored on devices where the risk of exposure is particularly high – such as a portable devices.

18.2.2. Measures to protect the confidentiality, integrity and availability of personal data

Confidentiality refers to the assurance that information is accessible only to authorised parties, integrity to the assurance that information remains accurate, and availability to the assurance that the information can be viewed whenever necessary.

When it comes to confidentiality, there are two things you must look at: how to prevent criminal hackers from breaking into your systems, and how to prevent your employees from exposing sensitive information.

The first issue can be addressed with defences such as anti-malware software, staff awareness training and vulnerability scans.

Meanwhile, you can reduce the risk of insider misuse by creating strict policies on data handling (with

an emphasis on disposing of information properly and implementing appropriate defences when data is stored in the Cloud), as well as measures to prevent employees from misusing information maliciously.

Data integrity can be ensured with measures such as access controls and audit trails, and data availability with a robust BCMS (business continuity management system).

18.2.3. Measures to restore data in the event of a disruption

In the event of a physical or technical incident that affects your ability to operate, you must be capable of restoring access to personal data promptly. You can do this by creating and regularly maintaining off-site backups, which will prevent data loss. This should be complemented by an incident response plan, which ensures that you can switch to backups with minimal delay.

18.2.4. Regularly test the effectiveness of these measures

You must be confident that the technical and organisational measures that you've adopted continue to work as intended. This might be a problem if the organisational structure has changed, rendering certain processes no longer relevant.

Alternatively, a review of your measures might reveal that a process isn't being followed properly, the technology is faulty or the risk has evolved.

Whatever the issue might be, you must regularly test any technical or organisational measure that you adopt. This might come in the form of an audit, a vulnerability scan or a penetration test, for example.

18.3. GDPR Article 32 checklist

To help you stay on top of your Article 32 obligations, the UK's data protection authority, the ICO (Information Commissioner's Office), has created a compliance checklist.

- Review the state of the art and costs of implementation when considering information security measures.
- Create an information security policy to keep track of technical and organisational measures.
- Create additional, specific policies to address information security measures.
- Regularly review policies to ensure they work as intend, and improve them where possible.
- Implement basic technical controls such as those specified by established frameworks such as Cyber Essentials.
- Assess whether new measures need to be implemented if the circumstances of data processing

change.

- Implement measures to protect the confidentiality, integrity and availability of personal data.
- Implement measures to restore access to personal data in the event of disruption.
- Regularly test and review technical and organisational measures, highlighting areas for improvement.
- Where appropriate, implement measures that adhere to an approved code of conduct or certification mechanism.
- Ensure that any data processor also implements appropriate technical and organisational measures.

19. GDPR data transfer rules

If you're transferring data outside of the EEA, the GDPR (General Data Protection Regulation) imposes some restrictions.

These apply to all data transfers, no matter the size of the transfer or how often you carry them out.

So how do you make a restricted transfer in accordance with the GDPR? We explain in this post.

19.1. How do I know if I'm making a restricted transfer?

Transfers of personal data are defined as restricted if:

- The GDPR applies to your processing of the personal data you are transferring.
- You are sending personal data (or making it accessible) to a receiver to which the GDPR does not apply. This usually applies to recipients located in a country outside the EEA.
- The receiver is a separate organisation or individual. This includes transfers to another company within the same corporate group.

19.2. How to make a restricted transfer in accordance with the GDPR?

To comply with the GDPR, you must consider the following factors:

19.2.1. Is the restricted transfer covered by an 'adequacy decision'?

If you are making a restricted transfer, you need to know whether it is covered by an EU Commission "adequacy decision".

The ICO describes the 'adequacy decision' as:

“...a finding by the Commission that the legal framework in place in that country, territory, sector or international organisation provides 'adequate' protection for individuals' rights and freedoms for their personal data.

19.2.2. Is the restricted transfer covered by appropriate safeguards?

If there is no 'adequacy decision' for your restricted transfer, you need to find out whether you can make the transfer subject to 'appropriate safeguards' listed in the GDPR.

These ‘appropriate safeguards’ are:

- A legally binding and enforceable instrument between public authorities or bodies.
- Binding corporate rules.
- Standard data protection clauses adopted by the Commission.
- Standard data protection clauses adopted by a supervisory authority and approved by the Commission.
- An approved code of conduct together with binding and enforceable commitments of the receiver outside the EEA.
- Certification under an approved certification mechanism together with binding and enforceable commitments of the receiver outside the EEA.
- Contractual clauses authorised by a supervisory authority.
- Administrative arrangements between public authorities or bodies which include enforceable and effective rights for the individuals whose personal data is transferred, and which have been authorised by a supervisory authority.

19.2.3. Is the restricted transfer covered by an exception?

If you are making a restricted transfer that isn’t covered by an ‘adequacy decision’ or the appropriate safeguards listed above, you can only the transfer if it is covered by one of the eight ‘exceptions’ set out in Article 49 of the GDPR.

These exceptions are:

- Exception 1: The individual has given his or her explicit consent to the restricted transfer.
- Exception 2. You have a contract with the individual and the restricted transfer necessary for you to perform that contract.

OR

You are about to enter into a contract with the individual, and the restricted transfer necessary for you to take steps requested by the individual to enter into that contract.

- Exception 3: You have (or are you entering into) a contract with an individual which benefits another individual whose data is being transferred, and that transfer necessary for you to either enter into that contract or perform that contract.

- Exception 4: You need to make the restricted transfer for important reasons of public interest.
- Exception 5: You need to make the restricted transfer to establish if you have a legal claim, to make a legal claim or to defend a legal claim.
- Exception 6: You need to make the restricted transfer to protect the vital interests of an individual. He or she must be physically or legally incapable of giving consent.
- Exception 7: You are making the restricted transfer from a public register.
- Exception 8: you are making a one-off restricted transfer, and it is in your compelling legitimate interests.

19.3. Pseudonymisation and encryption

The GDPR advises organisations to pseudonymise and/or encrypt all personal data.

This won't stop malicious actors accessing the information altogether, but it will make it much harder for them.

Pseudonymisation masks data by replacing identifying information with artificial identifiers.

Although it is central to protecting data – being mentioned 15 times in the GDPR – and can help protect the privacy and security of personal data, pseudonymisation has its limits, which is why the GDPR also mentions encryption.

Encryption also obscures information by replacing identifiers with something else.

But whereas pseudonymisation allows anyone with access to the data to view part of the data set, encryption allows only approved users to access the full data set.

Pseudonymisation and encryption can be used simultaneously or separately, and although neither requires technical knowledge to implement, the difficulty for organisations is in putting in place suitable security policies and procedures and making staff aware of their obligations.

19.4. What about the Schrems II ruling?

In July 2020, the ECJ (European Court of Justice) declared that the EU–US Privacy Shield – which organisations had used to make transatlantic personal data transfers – was no longer valid.

The decision came in the wake of complaints from the Austrian privacy activist Max Schrems, who argued that the US government's mass surveillance practices contradict the protections that the Privacy

Shield was supposed to provide.

The 5,000 or so organisations that currently use the framework will now have to rely on SCCs (standard contractual clauses), which are legal contracts that outline the terms and conditions for data transfers.

Schrems also challenged the validity of these, and although the ECJ chose not to abolish them, it did restrict their applicability.

Organisations and regulators must conduct case-by-case analyses of SCCs to determine whether protections concerning government access to data meet EU standards.

This will be a difficult task for all organisations, because to avoid a GDPR violation, you will need expert guidance.

20. 7 steps to highly effective GDPR compliance

The GDPR (General Data Protection Regulation) hasn't exactly crept up unnoticed over the past year or so, but it's still caught many organisations by surprise.

Some mistakenly thought that it would only affect large organisations, others doubted that the much-discussed massive fines would ever be issued, and a few thought that Brexit would save them from the EU regulation.

But none of those things are true. Organisations of all sizes have been put under regulatory pressure, and the ICO (Information Commissioner's Office) has already stated its intention to issue fines totalling £282 million against British Airways and Marriott International.

Meanwhile, although the specifics of Brexit are still unclear, one thing is certain: whatever happens, UK-based organisations will be subject to the GDPR's requirements. That's because the government adopted a UK-specific version of the Regulation's requirements as part of the DPA (Data Protection Act) 2018.

If you're overwhelmed about GDPR compliance or find most implementation advice too technical and complex, don't worry. IT Governance has created a simple guide to help you understand how to achieve regulatory compliance and avoid disciplinary action.

The first thing to remember is that the ICO will show leniency to organisations that can demonstrate that they are making efforts to achieve compliance. That means that simply beginning to take steps will help your standing should you come under investigation.

But exactly how should you proceed? Let's take a look.

20.1. Assess your current data protection measures

The first thing you should do is work out the extent to which you're already complying with the GDPR.

You're probably meeting some of the Regulation's requirements already, albeit in an unfocused way, so the scale of the task won't be quite as big as you might have feared.

There will, of course, be many areas where you aren't compliant. You can determine these by carrying out a gap analysis. This process identifies where your existing processes fall short of the Regulation's requirements and helps you understand what you need to do to bring them up to standard.

20.2. Identify and minimise risks that result from your data processing

The GDPR requires you to implement “appropriate technical and organisational measures” to ensure the security and privacy of the personal data your organisation processes.

To determine what’s appropriate, you should conduct a risk assessment. Only by evaluating the threats you face and your ability to deal with them can you establish a level of security that can adequately protect your organisation’s information assets in line with the GDPR – while keeping your expenditure within budget.

20.3. Educate and empower your employees to make better decisions

The GDPR requires every employee with permanent or regular access to personal data to receive appropriate data protection training.

Beyond this requirement, it’s important to recognise that information security is a responsibility for every employee, regardless of their level of access to personal data.

As well as ensuring that all your staff have a good understanding of the GDPR and information security, you’ll benefit from having a few individuals with more in-depth knowledge.

Some organisations will be required to appoint a DPO (Data Protection Officer), who provides an independent assessment of the organisation’s GDPR compliance activities. Organisations should also encourage managers and those closely involved with data processing to take advanced GDPR training courses.

20.4. Develop controls, policies and processes

GDPR compliance is too complex to maintain without a formal structure – especially as the Regulation places such a strong emphasis on documentation. Article 30, for example, requires data controllers to keep written records of data processing activities, including:

- The name and contact details of the controller and, where applicable, the joint controller, the controller’s representative and the Data Protection Officer;
- The purposes of the processing;
- A description of the categories of data subjects and of the categories of personal data; and

- The categories of recipients to whom the personal data have been or will be disclosed.

It's also a good idea to keep written records of the lawful basis for processing and data processor agreements.

20.5. Implement a DPIA

DPIAs (data protection impact assessments) are a form of risk assessment that identify any compliance issues that might arise as a result of data processing.

They are a useful accountability tool when it comes to GDPR compliance, as the results help you demonstrate that you have taken the appropriate technical and organisational measures required by the Regulation.

It's particularly important to carry out a DPIA when introducing new processes, systems or technologies for processing personal data.

20.6. Manage and respond to DSARs

Article 15 of the GDPR grants data subjects the right to access their personal data from data controllers so that they can understand – and check the lawfulness of – how it is processed.

A request to access personal data is known as a DSAR (data subject access request), sometimes referred to as a SAR.

Access requests are not new, but the GDPR introduced changes that make responding to them more challenging.

For example, organisations may no longer charge a fee, except in certain circumstances, and now have less time to respond – one calendar month rather than 40 days.

DSARs do not have to be made in writing, and can be made to any member of staff, so it's essential to ensure that everyone in your organisation can recognise a DSAR when they receive one. You should also have a proper procedure in place that every staff member can follow.

20.7. Plan, monitor and maintain a concrete GDPR compliance programme

GDPR compliance is ongoing, not a one-off task. Merely having the right procedures in place does not mean you are – and will remain – compliant.

You need to regularly monitor and audit your compliance. This means documenting your processes and procedures, and regularly checking them to ensure they're still fit for purpose, in line with the Regulation's accountability principle.

21. 5 things HR departments need to know about data protection

HR plays a crucial role in an organisation's GDPR (General Data Protection Regulation) compliance.

The department is full of personal data, whether it's of employees, their next of kin or candidates responding to job adverts.

With such an active role in processing sensitive information, HR staff must make sure they're doing everything necessary to protect employees and meet their regulatory requirements.

Let's take a look at five issues that HR must address when handling personal data.

21.1. Lawful basis for processing

An organisation must always document the reason it's processing personal data. The GDPR outlines six lawful bases that will be appropriate in different circumstances:

- Consent: the individual agrees to the data processing.
- A contract with the individual: for example, to supply goods or services they have requested, or to fulfil an obligation under an employee contract.
- Compliance with a legal obligation: when processing data for a particular purpose is a legal requirement.
- Vital interests: for example, when processing data will protect someone's physical integrity or life (either the data subject's or someone else's).
- A public task: for example, to complete official functions or tasks in the public interest. This will typically cover public authorities such as government departments, schools and other educational institutions; hospitals; and the police.
- Legitimate interests: when a private-sector organisation has a genuine and legitimate reason (including commercial benefit) to process personal data without consent, provided it is not outweighed by negative effects to the individual's rights and freedoms.

Before the GDPR, consent was considered the easiest way to process personal data lawfully, but the Regulation has not only toughened consent requirements but also made it impossible for organisations to use consent to collect employees' personal data.

That's because it states that consent can't be freely given if there's an imbalance of power, which would be the case between an employee and employer.

HR departments must therefore seek an alternative legal basis, the most appropriate generally being contractual necessity, a legal obligation or legitimate interests.

21.2. Data subject rights

They may be colleagues, but when it comes to their personal data, you must treat everyone in your organisation as data subjects in the same way as you would with customers or clients.

That means making them aware of their rights concerning the way your organisation processes personal information. There are eight data subject rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights related to automated decision making, including profiling

The right of access is by far the most commonly accessed, because employees tend to review the way an organisation processes their data before lodging a complaint.

Your data protection policy must state that employees are welcome to submit a DSAR (data subject access request) and explain how they can do this.

There shouldn't be a formal process; any written or verbal DSAR will do, even if it's as simple as an employee saying, 'I'd like to see what data you're keeping on me'.

As such, everyone in the HR department should be trained to recognise when a request has been made and the process they should follow to ensure they get the requisite information and respond within the one-month deadline.

21.3. Job applications

HR departments receive vast amounts of personal data whenever they post a job opening. CVs or applications will contain names, addresses, email addresses and employment history.

As with employee data, you must explain both your lawful basis for processing and how applicants can exercise their data subject rights. You could put this on the application form or link to it on your job posting.

Although the documentation process should be relatively straightforward – it's generally accepted that you need to provide personal details when applying for a job – you should pay attention to data retention.

The GDPR states that organisations can only keep personal data for as long as it's necessary for the purpose that it was collected. UK employers are legally required to hold on to job applications for six months, in case a candidate lodges a discrimination case.

However, you might want to retain data for longer than this – for example, if an applicant is unsuccessful on this occasion but might be suitable for future roles. This is an example of legitimate interests, and your data retention policy should state this if there's a chance that you might want to hold on to applications.

21.4. Acceptable use

There's a good chance your organisation already has an acceptable use policy. They clearly explain that employees are supposed to be spending their time in the office working, giving employers reasonable grounds to discipline or punish those who don't spend enough time doing their job.

But those who ignore this policy are not only slacking off but also potentially jeopardising the organisation's security.

Many of the disreputable websites that organisations ban are renowned sources of malware and viruses, which can cripple networks or, in the case of keyloggers, surreptitiously siphon sensitive information.

Employees should also be instructed not to download files from untrustworthy sites or their personal email accounts. The organisation's spam filters and anti-malware technology don't extend to personal emails, so it only takes one employee clicking a phishing email to infect the whole organisation.

You must therefore make it clear that acceptable use policies are as much about data protection as they are about ensuring a productive workforce.

21.5. Employee monitoring

Although organisations might be tempted to implement monitoring tools to make sure employees follow acceptable use policies, they should be very careful about how they do this.

Employers are entitled to keep an eye on what their staff do during office hours, but both CCTV footage and browser histories are considered personal data under the GDPR, so organisations need a lawful basis before processing it.

They must also be as deliberate and as unobtrusive as possible in their monitoring. Under no circumstances are employers justified in using exhaustive or automated monitoring methods (such as spyware) to look through an employee's browser history and workplace communications on the off-chance that they'll find evidence of misuse.

Employers should also refrain from methods that leave no trace of their monitoring, such as physically sitting at the employee's computer and looking through their private communications.

22. 72 hours and counting: Reporting Data Protection Breaches under the GDPR

The first 72 hours after you discover a data breach are critical.

Why? The GDPR (General Data Protection Regulation) requires all organisations to report certain types of personal data breach to the relevant supervisory authority.

More specifically, Article 33 says that, in the event of a personal data breach, data controllers should notify the appropriate supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it.

But how do you report a data breach, and what are the pitfalls when it comes to meeting this requirement?

In this post, we explain everything you need to know.

22.1. What is a data breach?

Let's start with the basics. The GDPR is concerned only with personal data – i.e. information that relates to a natural person, as opposed to company details. It's only when personal data is breached that you need to consider your GDPR compliance requirements.

But 'breach' here doesn't simply refer to cyber attacks. Article 4 of the Regulation

(<http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm>) defines a personal data breach as any event leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

As this definition suggests, data breaches aren't always a result of cyber criminals hacking into an organisation's systems. Breaches are just as likely to occur when an employee:

- Accidentally sends personal information to the wrong person;
- Accesses files that aren't relevant to their job function;
- Shares information with someone outside the organisation;
- Loses a device, such as a laptop, that contains personal information; or
- Fails to secure information online, making it publicly available.

Incidents that render organisations unable to access systems containing personal data are also considered data breaches, such as ransomware attacks or damaged hardware, because the information is no longer accessible.

22.2. When do data breaches need to be reported?

Data breaches only need to be reported if they “pose a risk to the rights and freedoms of natural living persons”.

This generally refers to the possibility of affected individuals facing economic or social damage (such as discrimination), reputational damage or financial losses.

Most data breaches fit into this category, but those that don’t include information that are linked to a specific individual are unlikely to pose a risk.

Whether you are required to report a data breach or not, the GDPR mandates that you keep a record of it.

22.3. Be wary of overreporting

Whether it’s due to misunderstanding the GDPR’s compliance or an abundance of caution, many organisations overlook the difference between recordable and reportable data breaches.

This is a trend that John Potts, Head of DPO, DSAR & Breach Support at [GRCILaw](https://www.grcilaw.com/topic/meet-the-team) (<https://www.grcilaw.com/topic/meet-the-team>), has noted since the GDPR took effect on 25 May 2018.

Speaking to IT Governance, he explained that organisations often report every incident they experience, because they “want to inform the ICO before someone else does, so they can get their side of the story in first.”

Potts acknowledges that it’s best to err on the side of caution if you’re unsure whether a data breach needs to be reported, but urges organisations to take the opportunity to consider this rather than going straight into reporting mode. The Information Commissioner’s Office help line is always on hand to offer advice.

Potts added that organisations should be concerned not only about over-reporting incidents but also what is initially reported.

“In my experience, the ICO appreciates that sometimes all the details of the breach may not be known at the initial stage of reporting. It is more important that the rights of the data subject are protected as

soon as possible rather than an organisation try to get their mitigation across to the ICO when they may not have a full picture,” he said.

“This desire to ‘fill in the form’ can lead to a knee-jerk reaction, meaning that the ICO and the organisation can go off on unnecessary avenues of investigations,” he added.

22.4. How to report a data breach?

Data breach notifications need to be sent to your supervisory authority. For organisations in the UK, this is the ICO.

Your report must contain:

- **Situational analysis:** You must provide as much context about the breach as possible. This includes the initial damage, how it affected your organisation, and what caused it.
- **Assessment of affected data:** You’ll need to determine the categories of personal data that has been breached, and the number of records affected.
- **Description of the impact:** Next, you’ll need to outline the consequences of the breach for affected parties. This will depend on the information that was compromised and if the data subject is aware of the breach
- **Report on staff training and awareness:** If the breach was a result of human error, you’ll need to disclose whether or not the employee(s) involved received data protection training in the past two years. If they have, you should provide details of your staff awareness training programme.
- **Preventive measures and actions:** Outline what (if any) preventative measures you had place before the breach occurred. You should also explain what steps have you taken, or plan to take, to mitigate the damage.
- **Oversight:** Finally, you’ll need to provide the contact details of your DPO (Data Protection Officer) or the person responsible for data protection.

The GDPR acknowledges that it may be difficult to produce this much information within 72 hours, but the important thing is to demonstrate that you’ve made progress.

You don’t need to be obsessed over an exact 72-hour deadline. It is far more important that the risks to the data subjects are addressed.

The timings of breaches are not an exact science; if you find yourself approaching the 72-hour

deadline, contact the ICO with the specific not speculative details that you have.

A swift response that's documented clearly but sent a few hours late is better than a shoddy response that was rushed in order to meet the disclosure deadline, Potts advises.

The emphasis is on protection of the rights and freedoms of the data subjects. Any breach that is likely to attract media interest should be reported to the ICO at the very earliest opportunity.

Potts concluded by reminding organisations that, although not covered specifically by the GDPR, in the event of a reportable breach they may have a legislative duty to inform other statutory bodies such as the CQC or if they are OES (operators of essential services) or an RSDPs (relevant digital service providers); under the Network and Information Systems Regulations 2018

(<http://www.legislation.gov.uk/ukxi/2018/506/contents>), they will need to report the breach to relevant regulatory body.

It's worth adding that your investigation can – and probably should – continue beyond the notification deadline.

More information will come to light as you analyse what went wrong and speak to those involved, and you can provide those details to the ICO where necessary.

22.5. What happens after you report an incident?

Once you've informed the ICO of the incident, you'll receive an automatic email to confirm receipt of your disclosure.

The incident will then go into a list of active cases that the ICO will look into to in due course. You will generally hear back quite quickly if the investigators are happy with your actions.

If the ICO suspects a GDPR violation, however, it may begin a formal investigation. These can take several months to complete, thanks to a backlog in cases and the back-and-forth nature of providing documentation and talking to relevant employees. In the event that the breach constitutes a criminal offence, they may instigate a criminal investigation.

That said, the ICO are likely to prioritise the case if the incident involves a serious breach affecting a lot of data subjects or is likely to attract media attention.

We've seen this already with July 2019's ruling on Marriott International's massive data breach. The breach was disclosed in November 2018, and the ICO came back with a verdict just over seven months

later, announcing its intention to fine the hotel chain £99 million.

22.6. What happens if you don't report an incident?

Failing to report an incident is a violation of the GDPR and is punishable by a fine.

That doesn't mean you should expect a barrage of financial penalties, though. The ICO has repeatedly said that fines will be a last resort and only issued for egregious or repeat offences.

That's not to say failure to notify won't come with any form of penalty.

The ICO can discipline organisations in other ways, such as enforcement actions and audits.

If this happens, your compliance measures will be scrutinised, weaknesses will be flagged and you'll be required to make the appropriate changes.

Some organisations have criticised this approach, saying that the data breach should be punishment enough.

However, Information Commissioner Elizabeth Denham insists

(<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/09/blog-gdpr-setting-the-record-straight-on-data-breach-reporting/>)

that the ICO's response measures aren't punishments.

“*The law is designed to push companies and public bodies to step up their ability to detect and deter breaches,*

What is foremost in regulators' minds is not to punish the organisations, but to make them better equipped to deal with security vulnerabilities.

We understand that there will [still] be attempts to breach organisations' systems, and that data breach reporting will not miraculously halt criminal activity. But the law will raise the level of security and privacy protections across the board.

23. 3 GDPR compliance tips for small businesses

This week marks one year since the GDPR (General Data Protection Regulation) took effect, and although we've seen organisations take huge strides in their commitment to information security, many are still struggling to implement the necessary measures.

Small businesses have faced the biggest challenge, partly because they lack the resources to overhaul their processes and invest in compliance solutions. However, regulatory compliance doesn't have to cost a fortune – in fact, some of the most effective steps are relatively simple and inexpensive.

23.1. GDPR compliance is only difficult if you don't understand what to do

The biggest blunders in data privacy (and the cause of many data breaches) comes from a basic lack of understanding of the GDPR's requirements.

So what should you do?

23.1.1. Take an online GDPR foundation training course

Online training provides a practical demonstration of the implications and legal requirements of the GDPR for organisations.

23.1.2. Get a 'how-to' guide as a reference

We recommend you keep a guidebook handy, which you can refer to when considering prospective data processing activities.

23.1.3. Keep an eye out for GDPR-related news.

Now that the Regulation is in full swing, there will be more cases of regulatory breaches and assessments of the way organisations fell short of their compliance requirements. By learning from others' mistakes, managers can get a better handle on the way the Regulation is interpreted and adapt their processes accordingly.

23.1.4. Teach your staff what they should and should not do

The next step is to make sure employees understand their data protection responsibilities. Most of your staff don't need to be GDPR experts, as they don't control the way data is used. However, they will almost certainly handle personal data or use systems that are designed to protect it. As such, there are certain requirements that employees need to be familiar with. Organisations can ensure everyone has this knowledge by conducting staff awareness training.

23.1.5. Enrol your team on an e-learning course

The most convenient way to deliver this training is through an e-learning course, because everyone will be given the same comprehensive training, which they can take at a time and place that suits them. All the organisation needs to do is send a course link to their staff and make sure everyone completes it. Likewise, the ease with which you can repeat courses makes e-learning ideal for training new starters, because you can simply direct them to the course rather than having to build GDPR training into their induction.

23.1.6. Place visual reminders in close proximity to staff

Office posters can ensure data protection and information security are at the forefront of your employees' minds.

23.1.7. Document everything to highlight your compliance efforts

A big stumbling block for a lot of organisations is keeping a record of everything they have done to mitigate their risks. The GDPR requires organisations to not only implement the necessary technical and organisational measures but also provide written proof of what they've done and why. This is so that organisations have better oversight of their data protection practices, which is helpful when it comes to reviewing their effectiveness. It also proves to supervisory authorities that the organisation is GDPR-compliant in the event of a regulatory investigation. Producing this information requires expert long-term planning, as there are dozens of documents you need to create and maintain indefinitely.

Employees responsible for documentation must be aware of what each document needs to contain.

24. Appendixes

24.1. Appendix A: The GDPR Compliance Quick Checklist

Obtain board-level support and establish accountability

- ☐ 1. Advise the board about data protection risks and the benefits of GDPR compliance.
- ☐ 2. Obtain management support for your GDPR compliance project.
- ☐ 3. Assign accountability for GDPR compliance to a director.

Scope and plan your GDPR compliance project

- ☐ 4. Appoint and train a project manager.
- ☐ 5. Appoint a data protection officer (DPO) if necessary.
- ☐ 6. Identify standards that could provide a framework to help you establish your compliance priorities, such as ISO 27001, ISO 27701 or BS 10012.
- ☐ 7. Assess whether data protection by design and by default has been incorporated into processes and systems.
- ☐ 8. Consider the implications of Brexit in your planning.

Conduct a data inventory and data flow audit

- ☐ 9. Assess the categories of data you hold, where the data comes from and the lawful basis for processing.
- ☐ 10. Create a map that shows how data flows to, through and from your organisation.
- ☐ 11. Use the data map to identify the risks in your data processing activities and determine whether a data protection impact assessment (DPIA) is required.
- ☐ 12. Create records of personal data processing activities, as required by Article 30, drawn from the data flow audit and gap analysis.

Undertake a comprehensive risk assessment

- ☐ 13. Establish the risk assessment plan.
- ☐ 14. Identify your risks.

- ☐ 15. Analyse and evaluate your risks.
- ☐ 16. Determine ways to control your risks.

Conduct a detailed gap analysis

- ☐ 17. Audit your current compliance position against the GDPR's requirements.
- ☐ 18. Determine which compliance gaps require remediation.

Develop operational policies, procedures and processes

- ☐ 19. Ensure your data protection policies and privacy notices are in line with the GDPR.
- ☐ 20. Where you rely on consent as your lawful basis for processing, ensure it meets the GDPR's requirements.
- ☐ 21. Review employee, customer and supplier contracts, and update them if necessary, to cover personal data processing.
- ☐ 22. Plan how to recognise and handle data subject access requests (DSARs) and provide responses within one calendar month.
- ☐ 23. Have a process in place for determining whether a DPIA is required.
- ☐ 24. Review whether your mechanisms for transferring data outside the EEA are compliant, especially after Brexit.

Secure personal data through procedural and technical measures

- ☐ 25. Have an information security policy in place.
- ☐ 26. Implement basic technical controls such as those specified by established frameworks like Cyber Essentials.
- ☐ 27. Use encryption and/or pseudonymisation where appropriate.
- ☐ 28. Ensure policies and procedures are in place to detect, report and investigate personal data breaches.

Ensure teams are trained and competent

- ☐ 29. Ensure internal communications with stakeholders and staff are effective.

- ☐ 30. Train your employees to understand the importance of data protection, basic GDPR principles and the procedures you have implemented to ensure compliance.

Monitor and audit compliance

- ☐ 31. Schedule regular audits of data processing activities and security controls.
- ☐ 32. Keep records of personal data processing up to date.
- ☐ 33. Undertake DPIAs where required.
- ☐ 34. Assess data protection practices and manage some of the more demanding elements of GDPR compliance.

24.2. Appendix B: The GDPR Compliance Checklist

Achieving GDPR Compliance shouldn't feel like a struggle. This is a basic checklist you can use to harden your GDPR compliancy.

If your organisation is determining the purpose of the storage or processing of personal information, it is considered a controller. If your organisation stores or processes personal data on behalf of another organisation, it is considered a processor. It is possible for your organisation to have both roles. Use the filter below to view only the relevant checklist items for your organisation.

This list is far from a legal exhaustive document (<https://gdpr-info.eu/>), it merely tries to help you overcome the struggle.

24.2.1. Select Your Role

- ☐ Data Controller: I determine why data is processed.
- ☐ Data Processor: I store or process data for someone else.
- ☐ Data Subject: My data is being stored or processed.

24.2.2. Data

- ☐ Your company has a list of all types of personal information it holds, the source of that information, who you share it with, what you do with it and how long you will keep it

(Data Processor , Data Controller)

This is a list of the actual types (columns) of information being held (eg Name, social security nr, address,...). For each type, a source should be documented, the parties this information is shared with, the purpose of the information and the duration for which the company will keep this information.

Reference:

- GDPR Article 30 – Records of processing activities
(<https://advisera.com/eugdpracademy/gdpr/records-of-processing-activities/>)

- ☐ Your company has a list of places where it keeps personal information and the ways data flows between them.

(Data Processor , Data Controller)

This could be a list of databases (eg Mysql), but it could also include offline datastores (paper).

Reference:

- GDPR Article 30 – Records of processing activities
(<https://advisera.com/eugdpracademy/gdpr/records-of-processing-activities/>)

- ☐ Your company has a publicly accessible privacy policy that outlines all processes related to personal data.

(Data Processor , Data Controller)

You should include information about all processes related to the handling of personal information. This document should include (or have links to) the types of personal information

the company holds, and where it holds them.

Reference:

- GDPR Article 30 – Records of processing activities
(<https://advisera.com/eugdpracademy/gdpr/records-of-processing-activities/>)

☐ Your privacy policy should include a lawful basis to explain why the company needs to process personal information.

(Data Controller)

It should contain a reason for data processing, eg the fulfillment of a contract.

Reference:

- GDPR Article 6 – Lawfulness of processing
(<https://advisera.com/eugdpracademy/gdpr/lawfulness-of-processing/>)

24.2.3. Accountability & Management

☐ Your company has appointed a Data Protection Officer (DPO).

(Data Processor , Data Controller)

A DPO is only required in three scenarios: (1) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (2) the core activities of the business consist of processing operations which, by virtue of their nature, scope, and/or purposes, require regular and systematic monitoring of data subjects on a large scale, or (3) the core activities of the business consist of processing on a large scale special categories of data (sensitive data) pursuant to Article 9 and personal data relating to criminal convictions or offenses pursuant to Article 10. If a DPO is required, the DPO should have knowledge of GDPR guidelines as well as knowledge about the internal processes that involve personal information.

Reference:

- GDPR Article 37 – Designation of the data protection officer

(<https://advisera.com/eugdpracademy/gdpr/designation-of-the-data-protection-officer/>)

- ☐ Create awareness among decision makers about GDPR guidelines.

(Data Processor , Data Controller)

Make sure key people and decision makers have up-to-date knowledge about the data protection legislation.

Reference:

- [GDPR Article 25 – Data protection by design and by default](#)

(<https://advisera.com/eugdpracademy/gdpr/data-protection-by-design-and-by-default/>)

- ☐ Make sure your technical security is up to date.

(Data Processor , Data Controller)

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Reference:

- GDPR Article 25 – Data protection by design and by default
(<https://advisera.com/eugdpracademy/gdpr/data-protection-by-design-and-by-default/>)

☐ Train staff to be aware of data protection.

(Data Processor)

A lot of security vulnerabilities involve cooperation of an unwitting person with access to internal systems. Make sure your employees are aware of these risks.

Reference:

- GDPR Article 25 – Data protection by design and by default
(<https://advisera.com/eugdpracademy/gdpr/data-protection-by-design-and-by-default/>)

☐ You have a list of sub-processors and your privacy policy mentions your use of this sub-processor.

(Data Processor)

You should inform your customers of the use of any sub-processor. They should consent by accepting your privacy policy.

Reference:

- GDPR Article 28 – Processor (<https://advisera.com/eugdpracademy/gdpr/processor/>)
- ComplianceRank - Keep track of the compliance of cloud services & subprocessors
(<https://www.compliancerank.com/>)

☐ If your business operates outside the EU, you have appointed a representative within the EU.

(Data Processor , Data Controller)

If you have a business outside of the EU and you collect data on EU citizens, you should assign a representative in one of the member states for your business. This person should handle all

issues related to processing. In particular, a local authority should be able to contact this person.

Reference:

- GDPR Article 27 – Representatives of controllers or processors not established in the Union
(<https://advisera.com/eugdpracademy/gdpr/representatives-of-controllers-or-processors-not-established-in-the-union/>)

- ☐ You report data breaches involving personal data to the local authority and to the people (data subjects) involved.

(Data Processor , Data Controller)

Personal data breaches should be reported within 72 hours to the local authority. You should report what data has been lost, what the consequences are and what countermeasures you have taken. Unless the data leaked was encrypted, you should also report the breach to the person (data subject) whose data you lost.

Reference: * GDPR Article 33 – Notification of a personal data breach to the supervisory authority

(<https://advisera.com/eugdpracademy/gdpr/notification-of-a-personal-data-breach-to-the-supervisory-authority/>)

* GDPR Article 34 – Communication of a personal data breach to the data subject

(<https://advisera.com/eugdpracademy/gdpr/communication-of-a-personal-data-breach-to-the-data-subject/>)

- ☐ There is a contract in place with any data processors that you share data with.

(Data Controller)

The contract should contain explicit instructions for the storage or processing of data by the processor. The contract should set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. For example, this could include a contract with your hosting provider. The same contract requirements apply when a processor engages a sub-processor to assist it in fulfilling processing activities on behalf of the controller.

Reference:

- GDPR Article 28 – Processor (<https://advisera.com/eugdpracademy/gdpr/processor/>)
- GDPR Article 29 – Processing under the authority of the controller or processor (<https://advisera.com/eugdpracademy/gdpr/processing-under-the-authority-of-the-controller-or-processor/>)
- ComplianceRank - Track hosting centers, DPAs & infrastructure partners from cloud services & subprocessors (<https://www.compliancerank.com/>)

24.2.4. New Rights

- ☐ Your customers can easily request access to their personal information.

(Data Processor , Data Controller)

If you do not already have a process defined for this, we've made an easy online form below.

Reference:

- GDPR Article 15 – Right of access by the data subject (<https://advisera.com/eugdpracademy/gdpr/right-of-access-by-the-data-subject/>)

- ☐ Your customers can easily update their own personal information to keep it accurate.

(Data Processor , Data Controller)

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (...)

Reference:

- GDPR Article 16 – Right to rectification (<https://advisera.com/eugdpracademy/gdpr/right-of-access-by-the-data-subject/>)

- ☐ You automatically delete data that your business no longer has any use for.

(Data Processor , Data Controller)

You should automate deletion of data you no longer need. For example, you should automatically delete data for customers whose contracts have not been renewed.

Reference:

- GDPR Article 5 – Principles relating to processing of personal data
(<https://advisera.com/eugdpracademy/gdpr/principles-relating-to-processing-of-personal-data/>)

- ☐ Your customers can easily request deletion of their personal data.

(Data Processor , Data Controller)

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (...)

Reference:

GDPR Article 17 – Right to erasure ('right to be forgotten')
(<https://advisera.com/eugdpracademy/gdpr/right-to-erasure-right-to-be-forgotten/>)

- ☐ Your customers can easily request that you stop processing their data.

(Data Processor , Data Controller)

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (...)

Reference:

- GDPR Article 18 – Right to restriction of processing

(<https://advisera.com/eugdpracademy/gdpr/right-to-restriction-of-processing/>)

- ☐ Your customers can easily request that their data be delivered to themselves or a 3rd party.

(Data Processor , Data Controller)

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (...)

Reference:

- GDPR Article 20 – Right to data portability
(<https://advisera.com/eugdpracademy/gdpr/right-to-data-portability/>)

- ☐ Your customers can easily object to profiling or automated decision making that could impact them.

(Data Controller)

This is only applicable if your company does profiling or any other automated decision making.

Reference:

- Article 22 – Automated individual decision-making, including profiling
(<https://advisera.com/eugdpracademy/gdpr/automated-individual-decision-making-including-profiling/>)

24.2.5. Consent

- ☐ Where processing is based on consent, such consent must be freely given, specific, informed, and revocable.

(Data Controller)

If your website collects personal information in some way, you should have an easily visible link to your privacy policy and confirm that the user accepts your terms and conditions. Consent requires an affirmative action, so pre-ticked boxes are not permitted.

Reference:

- [GDPR Article 7 – Conditions for consent](https://advisera.com/eugdpracademy/gdpr/conditions-for-consent/)
(<https://advisera.com/eugdpracademy/gdpr/conditions-for-consent/>)

- ☐ Your privacy policy should be written in clear and understandable terms.

(Data Controller)

It should be written in clear and simple terms and not conceal its intent in any way. Failing to do so could void the agreement entirely. When providing services to children, the privacy policy should be easy enough for them to understand.

Reference:

- [GDPR Article 7.2 – Conditions for consent](https://advisera.com/eugdpracademy/gdpr/conditions-for-consent/)
(<https://advisera.com/eugdpracademy/gdpr/conditions-for-consent/>)

- ☐ It should be as easy for your customers to withdraw consent as it was to give it in the first place.

(Data Controller)

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Reference:

- GDPR Article 7.2 – Conditions for consent
(<https://advisera.com/eugdpracademy/gdpr/conditions-for-consent/>)

☐ If you process children's personal data, verify their age and ask consent from their legal guardian.

(Data Controller)

For children younger than 16, you need to make sure a legal guardian has given consent for data processing. If consent is given via your website, you should try to make sure approval was actually given by the legal guardian (and not by the child).

Reference:

- GDPR Article 8 – Conditions applicable to child's consent in relation to information society services
(<https://advisera.com/eugdpracademy/gdpr/conditions-applicable-to-childs-consent-in-relation-to-information-society-services/>)

☐ When you update your privacy policy, you inform existing customers.

(Data Controller)

For example, by emailing upcoming changes of your privacy policy. Your communication should explain in a simple way what has changed.

Reference:

- GDPR Article 7 – Conditions for consent

24.2.6. Follow-up

- ☐ You regularly review policies for changes, effectiveness, changes in handling of data and changes to the state of affairs of other countries your data flows to.

(Data Controller)

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

You should follow up on best practices and changes to the policies in your local environment.

Reference:

- GDPR Article 25 – Data protection by design and by default
(<https://advisera.com/eugdpracademy/gdpr/data-protection-by-design-and-by-default/>)
- ComplianceRank - Track hosting centers, DPAs & infrastructure partners from cloud services & subprocessors (<https://www.compliancerank.com/>)

24.2.7. Special Cases

- ☐ Your business understands when you must conduct a DPIA for high-risk processing of sensitive

data.

(Data Controller)

This is only applies to businesses carrying out large-scale data processing, profiling and other activities with high risk to the rights and freedoms of people. A special assessment should be carried out in these cases.

Reference:

- DPIA according to the Dutch local authority (Dutch)
(<https://advisera.com/eugdpracademy/gdpr/data-protection-impact-assessment/>)
- GDPR Article 35 – Data protection impact assessment
(<https://advisera.com/eugdpracademy/gdpr/data-protection-impact-assessment/>)

☐ You should only transfer data outside of the EU to countries that offer an appropriate level of protection.

(Data Processor , Data Controller)

You should also disclose these cross-border data flows in your privacy policy.

Reference:

- GDPR Article 45 - Transfers on the basis of an adequacy decision
(<https://advisera.com/eugdpracademy/gdpr/transfers-on-the-basis-of-an-adequacy-decision/>)
- ComplianceRank - Track hosting center locations & hosting partners from cloud services & subprocessors (<https://www.compliancerank.com/>)

24.2.8. User Rights

☐ Right to receive transparent information, communication and modalities for the exercise of your rights.

(Data Subject)

The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to you in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by you, the information may be provided orally, provided that your identity is proven by other means.

Reference:

- GDPR Article 12 - Transparent information, communication and modalities for the exercise of the rights of the data subject (<https://gdpr-info.eu/art-12-gdpr/>)

☐ Right to receive specific information when your personal data are collected from you directly.

(Data Subject)

This information is : 1) The identity and the contact details of the controller and, where applicable, of the controller's representative. 2) The contact details of the data protection officer, where applicable. 3) The purposes of the processing for which the personal data are intended as well as the legal basis for the processing. 4) Where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party. 5) The recipients or categories of recipients of the personal data, if any. 6) Where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Reference:

- GDPR Article 13 - Information to be provided where personal data are collected from the data subject (<https://gdpr-info.eu/art-13-gdpr/>)

☐ Right to receive specific information when your personal data are not collected from you directly.

(Data Subject)

This information is : 1) The identity and the contact details of the controller and, where applicable, of the controller's representative. 2) The contact details of the data protection officer, where applicable. 3) The purposes of the processing for which the personal data are intended as well as the legal basis for the processing. 4) The categories of personal data concerned. 5) The recipients or categories of recipients of the personal data, if any. 6) Where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

Reference:

- GDPR Article 14 - Information to be provided where personal data have not been obtained from the data subject (<https://gdpr-info.eu/art-14-gdpr/>)

☐ Right of access: You have the right to obtain from the controller confirmation as to whether or not your personal data are being processed, and, where that is the case, access to your personal data.

(Data Subject)

You also have to right to access the following information: 1) The purposes of the processing. 2) The categories of personal data concerned. 3) The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations. 4) Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period. 5) The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing. 6) The right to lodge a complaint with a supervisory authority. 7) Where the personal data are not collected from the data subject, any available information as to their source. 8) The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Reference:

- GDPR Article 15 - Right of access by the data subject (<https://gdpr-info.eu/art-15-gdpr/>)

☐ Right to rectification: You have the right to obtain from the controller without undue delay the rectification of inaccurate personal data.

(Data Subject)

Taking into account the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Reference:

- GDPR Article 16 - Right to rectification (<https://gdpr-info.eu/art-16-gdpr/>)

☐ Right to erasure: You have the right to obtain from the controller the erasure of your personal data without undue delay.

(Data Subject)

The controller shall have the obligation to erase your personal data without undue delay where one of the following grounds applies: 1) The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. 2) The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing. 3) The data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2). 4) The personal data have been unlawfully processed. 5) The personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject. 6) The personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Reference:

- GDPR Article 17 - Right to erasure ('right to be forgotten') (<https://gdpr-info.eu/art-17-gdpr/>)

☐ Right to restriction of processing: You have the right to obtain from the controller restriction of processing.

(Data Subject)

This right applies in the following situations: 1) The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data. 2) The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead. 3) The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims. 4) The data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

Reference:

- GDPR Article 18 - Right to restriction of processing (<https://gdpr-info.eu/art-18-gdpr/>)

☐ Right to be notified regarding rectification or erasure of your personal data or restriction of

processing: The controller shall communicate any rectification or erasure of your personal data or restriction of processing.

(Data Subject)

This right is carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform you about those recipients if you requests it.

Reference:

- GDPR Article 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing (<https://gdpr-info.eu/art-19-gdpr/>)

☐ Right to portability: You have the right to receive your personal data, which you have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which your personal data have been provided.

(Data Subject)

This processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and the processing is carried out by automated means.

Reference:

- GDPR Article 20 - Right to data portability (<https://gdpr-info.eu/art-20-gdpr/>)

☐ Right to object: You have the right to object, on grounds relating to your particular situation, at any time to processing of your personal data which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions.

(Data Subject)

The controller shall no longer process your personal data unless the controller demonstrates compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

Reference:

- GDPR Article 21 - Right to object (<https://gdpr-info.eu/art-21-gdpr/>)

☐ Right not to be subject to a decision based solely on automated processing: You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects you.

(Data Subject)

This does not apply if the decision: 1) is necessary for entering into, or performance of, a contract between the data subject and a data controller. 2) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. 3) is based on the data subject's explicit consent.

Reference:

- GDPR Article 22 - Automated individual decision-making, including profiling
(<https://gdpr-info.eu/art-22-gdpr/>)

24.3. Appendix C: Sample DPIA Questionnaire

You should start to fill out the Questionnaire at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO	

Step 1: Identify the need for a DPIA

<p>Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal.</p> <p>Summarise why you identified the need for a DPIA.</p>

Step 2: Describe the processing

Describe the nature of the processing:	<ul style="list-style-type: none">• How will you collect, use, store and delete data?• What is the source of the data?• Will you be sharing data with anyone?• What types of processing identified as likely high risk are involved?
---	---

Describe the scope of the processing:

- What is the nature of the data, and does it include special category or criminal offence data?
- How much data will you be collecting and using?
- How often? How long will you keep it?
- How many individuals are affected? What geographical area does it cover?

Describe the context of the processing:

- What is the nature of your relationship with the individuals?
- How much control will they have?
- Would they expect you to use their data in this way?
- Do they include children or other vulnerable groups?
- Are there prior concerns over this type of processing or security flaws?
- Is it novel in any way?
- What is the current state of technology in this area?
- Are there any current issues of public concern that you should factor in?
- Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing:

- What do you want to achieve?
- What is the intended effect on individuals?
- What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

<p>Consider how to consult with relevant stakeholders:</p>	<ul style="list-style-type: none">• Describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so.• Who else do you need to involve within your organisation?• Do you need to ask your processors to assist?• Do you plan to consult information security experts, or any other experts?
---	---

Step 4: Assess necessity and proportionality

<p>Describe compliance and proportionality measures, in particular:</p>	<ul style="list-style-type: none">• What is your lawful basis for processing?• Does the processing actually achieve your purpose?• Is there another way to achieve the same outcome?• How will you prevent function creep?• How will you ensure data quality and data minimisation?• What information will you give individuals?• How will you help to support their rights?• What measures do you take to ensure processors comply?• How do you safeguard any international transfers?
--	---

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Measures approved by:	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:	
DPO advice accepted or overruled by:	If overruled, you must explain your reasons
Comments:	
Consultation responses reviewed by:	If your decision departs from individuals' views, you must explain your reasons
Comments:	
This DPIA will kept under review by:	The DPO should also review ongoing compliance with DPIA

24.4. Appendix D: Privacy Policy Template

YOUR_COMPANY_NAME

PRIVACY POLICY

ACCOUNT_JOB_COMPANY (the “Company”) respects the privacy of its online visitors and customers of its products and services (including, but not limited to QiCYCLE) and complies with applicable laws for the protection of your privacy, including, without limitation, the European Union General Data Protection Regulation ("GDPR") and the Swiss and EU Privacy Shield Frameworks.

1. Definitions

Wherever we talk about Personal Data below ("Personal Data"), we mean any information that can either itself identify you as an individual ("Personally Identifying Information") or that can be connected to you indirectly by linking it to Personally Identifying Information, for example:

- (i) your account registration information on our website and in our App;
- (ii) when you request any support from us or report any problem to us;
- (iii) information provided from using certain services or features;
- (iv) information from completion of survey or questionnaire;
- (v) technical information, including the Internet protocol (IP) address used
- (vi) and your log-in information, browser, time zone setting, browser plug-in types and versions, operating system and platform;
- (vii) details of any transactions, purchases and payments you made;
- (viii) your general interaction with the website, including the full Uniform Resource Locators (URLs), clickstream to, through and from our site, products you viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information;
- (ix) information received from third parties, such as business partners, sub-contractors, payment and delivery services, referral by other users.

The Company also processes anonymous data, aggregated or not, to analyze and produce statistics related to the habits, usage patterns, and demographics of customers as a group or as individuals. Such anonymous data does not allow the identification of the customers to which it relates. the Company may share anonymous data, aggregated or not, with third parties. Please be aware that the Company may choose to permit third parties to offer subscription and/or registration-based services through the Company's site. The Company shall not be responsible for any actions or policies of such third parties and you should check the applicable privacy policy of such party when providing personally identifiable information.

By using the Company's website, you signify your assent to the Company's privacy policy. If you do not agree to this policy, please do not use the Company's website(s).

2. Why the Company Collects and Processes Data

The Company collects and processes Personal Data for the following reasons:

- (a) performing our agreement with you to provide content and services, including providing, improving and developing our services;
- (b) researching, designing and launching new features or products;
- (c) providing you with alerts, updates, materials or information about our services or other types of information that you requested or signed up to;
- (d) collecting overdue amounts;
- (e) responding or taking part in legal proceedings, including seeking professional advice, or for the purposes of the legitimate and legal interests of the Company or a third party (e.g. the interests of our other customers);
- (f) compliance with legal obligations that we are subject to;
- (g) communicating with you and responding to your questions or requests;
- (i) purposes directly related or incidental to the above; or
- (j) where you have given consent to it.

These reasons for collecting and processing Personal Data determine and limit what Personal Data we

collect and how we use it (section 3. below), how long we store it (section 4. below), who has access to it (section 5. below) and what rights and other control mechanisms are available to you as a user (section 6. below).

3. What Data We Collect and Process

3.1 Basic Account Data

When setting up an Account, the Company will collect your email address and country of residence. You are also required to choose a user name and a password. The provision of this information is necessary to register a User Account. You are responsible for keeping this password confidential. We ask you not to share a password with anyone.

During setup of your account, the account is automatically assigned a number (the "ID") that is later used to reference your user account without directly exposing Personally Identifying Information about you.

3.2 Transaction and Payment Data

In order to make a transaction online, you may need to provide payment data to the Company to enable the transaction. If you pay by credit card, you need to provide typical credit card information (name, address, credit card number, expiration date and security code) to the Company, which the Company will process and transmit to the payment service provider of your choice to enable the transaction and perform anti-fraud checks. Likewise, the Company will receive data from your payment service provider for the same reasons.

3.3 Other Data You Explicitly Submit

We will collect and process Personal Data whenever you explicitly provide it to us or send it as part of communication with others, e.g. in forums, chats, or when you provide feedback or other user generated content. This data includes:

- (a) Information that you post, comment or follow in any of our Content and Services;
- (b) Information sent through chat;
- (c) Information you provide when you request information or support from us or purchase Content and Services from us, including information necessary to process your orders with the relevant payment

merchant or, in case of physical goods, shipping providers;

(d) Information you provide to us when participating in competitions, contests and tournaments or responding to surveys, e.g. your contact details.

3.4 Your Use of the Websites

We collect a variety of information through your general interaction with the websites, Content and Services offered by us. Personal Data we collect may include, but is not limited to, browser and device information, data collected through automated electronic interactions and application usage data.

Likewise, we will track your process across your websites and applications to verify that you are not a bot and to optimize our services.

3.5 Your Use of Services and other Subscriptions

In order to provide you with services, we need to collect, store and use various information about your activity in our Content and Services. "Content-Related Information" includes your ID, as well as information about your preferences, progress, time spent, as well as information about the device you are using, including what operating system you are using, device settings, unique device identifiers, and crash data.

3.6 Tracking Data and Cookies

We use "Cookies", which are text files placed on your computer, to help us analyze how users use our services, and similar technologies (e.g. web beacons, pixels, ad tags and device identifiers) to recognize you and/or your device(s) on, off and across different devices and our services, as well as to improve the services we are offering, to improve marketing, analytics or website functionality. The use of Cookies is standard on the internet. Although most web browsers automatically accept cookies, the decision of whether to accept or not is yours. You may adjust your browser settings to prevent the reception of cookies, or to provide notification whenever a cookie is sent to you. You may refuse the use of cookies by selecting the appropriate settings on your browser. However, please note that if you do this, you may not be able to access the full functionality of our websites. When you visit any of our services, our servers log your global IP address, which is a number that is automatically assigned to the network your computer is part of.

3.7 Third Party Services

This website uses GoogleLogin, Facebook Login ("Third Party Service"). Third Party Service uses

"cookies", which are text files placed on visitors' computers, to help the website operators analyze how visitors use the site. The information generated by the cookie about the visitors' use of the website will generally be transmitted to and stored by Third Party Service on servers in the [United States]. Please be aware that Company cannot or does not control the use of cookies or the resulting information by the Third Party Service.

On behalf of the website operator, Third Party Service will use this information for the purpose of evaluating the website / location / credentials for its users, in order to compile reports on website activity, and to provide other services relating to website activity and internet usage for website operators.

Third Party Service will not associate the IP address transferred any other data held by the Company. You may refuse the use of cookies by selecting the appropriate settings on your browser. However, please note that in this case you may not be able to use the full functionality of this website.

3.8 Content Recommendations

We may process information collected under this section 3 so that content, products and services shown on the pages and in update messages displayed when launching the service can be tailored to meet your needs and populated with relevant recommendations and offers. This is done to improve your customer experience.

Subject to your separate consent or where explicitly permitted under applicable laws on email marketing, the Company may send you marketing messages about products and services offered by the Company to your email address. In such a case we may also use your collected information to customise such marketing messages as well as collect information on whether you opened such messages and which links in their text you followed.

You can opt out or withdraw your consent to receive marketing emails at any time by either withdrawing the consent on the same page where you previously provided it or clicking the "unsubscribe" link provided in every marketing email. Notwithstanding any opt out of promotional or marketing emails by you, we reserve the right to contact you regarding account status, changes to the user agreement and other matters relevant to the underlying service and/or the information collected.

3.9 Information Required to Detect Violations

We collect certain data that is required for our detection, investigation and prevention of fraud, cheating and other violations of the applicable laws ("Violations"). This data is used only for the purposes of

detection, investigation, prevention and, where applicable, acting on of such Violations and stored only for the minimum amount of time needed for this purpose. If the data indicates that a Violation has occurred, we will further store the data for the establishment, exercise or defense of legal claims during the applicable statute of limitations or until a legal case related to it has been resolved. Please note that the specific data stored for this purpose may not be disclosed to you if the disclosure will compromise the mechanism through which we detect, investigate and prevent such Violations.

4. How We Store Data

4.1 Period of Storage

We will store your information as long as necessary to fulfil the purposes for which the information is collected and processed or — where the applicable law provides for longer storage and retention period — for the storage and retention period required by law. In particular, if you terminate your User Account, your Personal Data will be marked for deletion except to the degree legal requirements or other prevailing legitimate purposes dictate a longer storage. All your data and credits will be lost after deletion.

4.2 Deletion of Data

In cases where Personal Data cannot be completely deleted in order to ensure the consistency of the system, the user experience or the community, your information will be permanently anonymized. Please note that the Company is required to retain certain transactional data under statutory commercial and tax law for a period of up to ten (10) years.

If you withdraw your consent on which a processing of your Personal Data, we will delete your Personal Data without undue delay to the extent that the collection and processing of the Personal Data was based on the withdrawn consent.

If you exercise a right to object to the processing of your Personal Data, we will review your objection and delete your Personal Data that we processed for the purpose to which you objected without undue delay, unless another legal basis for processing and retaining this data exists or unless applicable law requires us to retain the data.

4.3 Location of Storage

The data that we collect from you may be transferred to, and stored at Hong Kong, or a destination outside of your jurisdiction. It may also be processed by third parties who operate outside of your

jurisdiction. By submitting your personal data you agree to this transfer, storing or processing of data outside of your jurisdiction. We will take all steps reasonably necessary to ensure that your data is treated securely in accordance with this privacy policy.

5. Who Has Access to Data

5.1 The Company and its subsidiaries may share your Personal Data with each other and use it to the degree necessary to achieve the purposes listed in section 2 above. This includes our overseas offices, affiliates, business partners and counterparts (on a need-to-know basis only). In the event of a reorganization, sale or merger we may transfer Personal Data to the relevant or proposed transferees of our operations (or a substantial part thereof) in any part of the world.

5.2 We may also share your Personal Data with our third party providers that provide customer support services in connection with goods, Content and Services distributed via us. Your Personal Data will be used in accordance with this Privacy Policy and only as far as this is necessary for performing customer support services.

5.3 We may also share your information with our personnel, agents, advisers, auditors, contractors, financial institutions, and service providers in connection with our operations or services (for example staff engaged in the fulfilment of your order, the processing of your payment and the provision of support services); persons under a duty of confidentiality to us; or persons to whom we are required to make disclosure under applicable laws and regulations in any part of the world.

5.4 In accordance with internet standards, we may also share certain information (including your IP address and the identification of content you wish to access) with our third party network providers that provide content delivery network services and server services in connection with us. Our content delivery network providers enable the delivery of digital content you have requested, by using a system of distributed servers that deliver the content to you, based on your geographic location.

5.5 The Company may allow you to link your User Account to an account offered by a third party. If you consent to link the accounts, the Company may collect and combine information you allowed the Company to receive from a third party with information of your User Account to the degree allowed by your consent at the time. If the linking of the accounts requires the transmission of information about your person from the Company to a third party, you will be informed about it before the linking takes place and you will be given the opportunity to consent to the linking and the transmission of your information. The third party's use of your information will be subject to the third party's privacy policy, which we encourage you to review.

5.6 The Company may release Personal Data to comply with court orders or laws and regulations that require us to disclose such information.

5.7 We make certain data related to your User Account available to other users. This information can be accessed by anyone by querying your ID. At a minimum, the public persona name you have chosen to represent you are accessible this way. The accessibility of any additional info about you can be controlled through your user profile page; data publicly available on your profile page can be accessed automatically. While we do not knowingly share Personally Identifying Information about you such as your real name or your email address, any information you share about yourself on your public profile can be accessed, including information that may make you identifiable.

5.8 The community includes message boards, forums and/or chat areas, where users can exchange ideas and communicate with each other. When posting a message to a board, forum or chat area, please be aware that the information is being made publicly available online; therefore, you are doing so at your own risk; and that such information can be collected, correlated and used by third parties and may result in unsolicited messages from other posters or third parties and these activities are beyond our control. If your Personal Data is posted on one of our community forums against your will, please use the reporting function and the help site to request its removal.

6. Your Rights and Control Mechanisms

You have the right to:

- (a) check whether we hold personal data about you;
- (b) access any personal data we hold about you;
- (c) require us to correct any inaccuracy or error in any personal data we hold about you;
- (d) request for the deletion of your personal data through the deletion of user account.

The data protection laws of the European Economic Area and other territories grant their citizens certain rights in relation to their Personal Data. While other jurisdictions may provide fewer statutory rights to their citizens, we make the tools designed to exercise such rights available to our customers worldwide.

As a resident of the European Economic Area you have the following rights in relation to your Personal Data:

6.1 Right of Access

You have the right to access your Personal Data that we hold about you, i.e. the right to require free of charge (i) information whether your Personal Data is retained, (ii) access to and/or (iii) duplicates of the Personal Data retained. You can use the right to access to your Personal Data through the Privacy Dashboard. If the request affects the rights and freedoms of others or is manifestly unfounded or excessive, we reserve the right to charge a reasonable fee (taking into account the administrative costs of providing the information or communication or taking the action requested) or refuse to act on the request.

6.2 Right to Rectification

If we process your Personal Data, we shall endeavor to ensure by implementing suitable measures that your Personal Data is accurate and up-to-date for the purposes for which it was collected. If your Personal Data is inaccurate or incomplete, you can change the information you provided via the Privacy Dashboard.

6.3. Right to Erasure

You have the right to obtain deletion by us of Personal Data concerning you by deleting your User Account via the support page.

As a result of deleting your User Account, you will lose access to services, including the User Account, Subscriptions and service-related information linked to the User Account and the possibility to access other services you are using the User Account for.

We allow you to restore your User Account during a grace period of 30 (thirty) days from the moment you request deletion of your User Account. This functionality allows you not to lose your account by mistake, because of your loss of your account credentials or due to hacking. During the suspension period, we will be able to finalize financial and other activities that you may have initiated before sending the User Account deletion request. After the grace period, Personal Data associated with your account will be deleted subject to section 4. above.

In some cases, deletion of your User Account, and therefore Personal Data deletion, is complicated. In some cases, considering the complexity and number of the requests, the period for Personal Data erasure may be extended, but for no longer than two further months.

6.4 Right to Object

When our processing of your Personal Data is based on legitimate interests according to Article 6(1)(f) of the GDPR / section 2.c) of this Privacy Policy, you have the right to object to this processing. If you object we will no longer process your Personal Data unless there are compelling and prevailing legitimate grounds for the processing as described in Article 21 of the GDPR; in particular if the data is necessary for the establishment, exercise or defense of legal claims.

You also have the right to lodge a complaint at a supervisory authority.

7. Children

The minimum age to create a User Account is 13. the Company will not knowingly collect Personal Data from children under this age. Insofar as certain countries apply a higher age of consent for the collection of Personal Data, the Company requires parental consent before a User Account can be created and Personal Data associated with it collected. The Company encourages parents to instruct their children to never give out personal information when online.

8. Contact Info

You can contact the Company's Data Protection Officer at the address below.

While we review any request sent by mail, please be aware that to combat fraud, harassment and identity theft, the only way to access, rectify or delete your data is through logging in with your User Account at privacy@meniny.cn.

ACCOUNT_JOB_ADDRESS_MULTI_LINE

Attention: Privacy Officer

9. Revision Date

This privacy policy was last updated on 24 April 2021 ("Revision Date"). If you were a user before the Revision Date, it replaces the existing Privacy Policy. The Company reserves the right to change this policy at any time by notifying the users of the existence of a new privacy statement. This policy is not intended to and does not create any contractual or legal rights in or behalf of any party.

24.5. Appendix E: Data Protection Policy Template

Data Protection Policy

Goal of the data protection policy

The goal of the data protection policy is to depict the legal data protection aspects in one summarising document. It can also be used as the basis for statutory data protection inspections, e.g. by the customer within the scope of commissioned processing. This is not only to ensure compliance with the European General Data Protection Regulation (GDPR) and Data protection Act (DPA) 2018 but also to provide proof of compliance.

Preamble

Brief description of the company and motivation to comply with data protection.

Security policy and responsibilities in the company

- For a company, in addition to existing corporate objectives, the highest data protection goals are to be defined and documented. Data protection goals are based on data protection principles and must be individually modified for every company.
- Determination of roles and responsibilities (e.g. representatives of the company, operational Data Protection Officers, coordinators or data protection team and operational managers)
- Commitment to continuous improvement of a data protection management system
- Training, sensitisation and obligation of the employees

Legal framework in the company

- Industry-specific legal or conduct regulations for handling personal data
- Requirements of internal and external parties
- Applicable laws, possibly with special local regulations

Documentation

- Conducted internal and external inspections
- Data protection need: determination of protection need with regard to confidentiality, integrity and

availability.

Existing technical and organisational measures (TOM)

Appropriate technical and organisational measures that must be implemented and substantiated, taking into account, inter alia, the purpose of the processing, the state of the technology and the implementation costs. The description of the implemented TOM can, for example, be based on the structure of ISO/IEC 27002, taking into account ISO/IEC 29151 (guidelines for the protection of personal data). The respective chapters should be substantiated by referencing the existing guidelines.

Examples of such guidelines include:

- Guideline for the rights of data subjects
- Access control
- Information classification (and handling thereof)
- Physical and environmental-related security for end users such as:
 - Permissible use of values
 - Guideline for information transfer based on the work environment and screen locks
 - Mobile devices and telecommuting
 - Restriction of software installation and use
- Data backup
- Information transfer
- Protection against malware
- Handling technical weak points
- Cryptographic measures
- Communication security
- Privacy and protection of personal information
- Supplier relationships: Noting regular inspection and evaluation of data processing, especially the efficacy of the implemented technical and organisational measures.

24.6. Appendix F: GDPR Data Map Template

GDPR Data Map

Filled By:


Date:

Version:

Source	Data	Reason	Handling	Erase	Subject is a Over	Consent Obtained	Mission Critical Data	Sensitive Data
How was this data collected? • Contact Form • External Organisation	What data are you collecting? • Email Address • IP Address • Ethnic Origin • Phone Number	Why're you collecting this data? • Marketing • CRM • Processing/Analytics	How you'll store the data? How it'll be processed? Who has access to it?	How long you'll keep the data? What is the criteria used to determine this period?				

Designed By: 李申翊

Version: 1.0.0

 QICYCLE
iding.cc

24.7. Appendix G: Records of Processing Activities for Data Controller Template

For Data Controller

Records of Processing Activities

Filled By:


For:

Date:

Contact	Categories	Purposes	Security	Recipients	Erasure	Sensitive Data
The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer.	A description of the categories of data subjects and of the categories of personal data.	Why're you collecting this data? <ul style="list-style-type: none">• Marketing• CRM• Processing/Analytics	Where possible, a general description of the technical and organisational security measures.	The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations.	How long you'll keep the data? What is the criteria used to determine this period?	

Designed By: 李申朗

Version: 1.0.0

Oqicycle
lliding.cc

24.8. Appendix H: Records of Processing Activities for Data Processor Template

For Data Processor

Records of Processing Activities

Filled By:


For:

Date:

Contact	Categories	Recipients	Security
The name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's representative, and the data protection officer;	The categories of processing carried out on behalf of each controller.	Where applicable, transfers of personal data to a third country or an international organisation and the documentation of suitable safeguards;	Where possible, a general description of the technical and organisational security measures.

Designed By: 李申朗

Version: 2.0.0

Oqicycle
lliding.cc

24.9. Appendix I: Categories of Personal Information

The following are categories of information relating to an individual, whether it relates to his or her private, professional or public life. Categories are not exclusive. Information may transcend multiple categories.

INTERNAL	
Knowledge and Belief	Information about what a person knows or believes
	religious beliefs, philosophical beliefs, thoughts, what they know and don't know, what someone thinks
Authenticating	Information used to authenticate an individual with something they know
	passwords, PIN, mother's maiden name
Preference	Information about an individual's preferences or interests
	opinions, intentions, interests, favorite foods, colors, likes, dislikes, music

EXTERNAL	
Identifying	Information that uniquely or semi-uniquely identifies a specific individual
	name, user-name, unique identifier, government issued identification, picture, biometric data
Ethnicity	Information that describes an individual's origins and lineage
	race, national or ethnic origin, languages spoken, dialects, accents
Sexual	Information that describes an individual's sexual life
	gender identity, preferences, proclivities, fetishes, history, etc.
Behavioral	Information that describes an individual's behavior or activity, on-line or off
	browsing behavior, call logs, links clicked, demeanor, attitude
Demographic	Information that describes an individual's characteristics shared with others
	age ranges, physical traits, income brackets, geographic
Medical and Health	Information that describes an individual's health, medical conditions or health care

EXTERNAL	
	physical and mental health, drug test results, disabilities, family or individual health history, health records, blood type, DNA code, prescriptions
Physical Characteristic	Information that describes an individual's physical characteristics
	height, weight, age, hair color, skin tone, tattoos, gender, piercings

HISTORICAL

Life History

Information about an individual's personal history

events that happened in a person's life, either to them or just around them which might have influenced them (WWII, 9/11)

TRACKING

Computer Device

Information about a device that an individual uses for personal use (even part-time or with others)

IP address, Mac address, browser fingerprint.

Contact

Information that provides a mechanism for contacting an individual

email address, physical address, telephone number

Location

Information about an individual's location

country, GPS coordinates, room number

FINANCIAL	
Account	Information that identifies an individual's financial account
	credit card number, bank account
Ownership	Information about things an individual has owned,
	rented, borrowed, possessed cars, houses, apartments, personal possessions
Transactional	Information about an individual's purchasing, spending or income
	purchases, sales, credit, income, loan records, transactions, taxes, purchases and spending habits
Credit	Information about an individual's reputation with regards to money
	credit records, credit worthiness, credit standing, credit capacity

SOCIAL	
Professional	Information about an individual's educational or professional career
	job titles, salary, work history, school attended, employee files, employment history, evaluations, references, interviews, certifications, disciplinary actions
Criminal	Information about an individual's criminal activity
	convictions, charges, pardons
Public Life	Information about an individual's public life
	character, general reputation, social status, marital status, religion, political affiliations, interactions, communications meta-data
Family	Information about an individual's family and relationships
	family structure, siblings, offspring, marriages, divorces, relationships
Social Network	Information about an individual's friends or social connections
	friends, connections, acquaintances, associations, group membership
Communication	Information communicated from or to an individual
	telephone recordings, voice mail, email



Everything You Need to Know About GDPR Compliance.

Made with ❤️ in Shenzhen



