Simplifying Compliance

P4P Compliance Management Limited

The General Data Protection Regulations (GDPR) Essentials

Image by DC Studio

Table of Contents

© 2023 P4P Compliance Management Limited

Introduction

This article has been produced to provide an overview of the key themes of The General Data Protection Regulation (GDPR).

Using plain and simple terminology, the document describes the absolutely necessary requirements UK businesses need to know, to help them comply with current data protection laws.

It includes links to relevant sections of the GDPR itself, and to The Information Commissioners Office (ICO), the UK's independent body set up to uphold information rights, the Data Protection Act 2018, Freedom of Information, Privacy and Electronic Communications Regulations.

The GDPR applied in the UK since 25 May 2018 replacing all previous data protection directive.

The GDPR affects any business that have day-to-day responsibility collects, processes, stores, and uses personal data from people residing in the UK, and to controllers and processors based outside the UK if their processing activities relate to:

- Offering goods or services to individuals in the UK
- Monitoring the behavior of individuals taking place in the UK

1st January 2021 the UK formally left the European Union (EU) and became known as a third country.

This led to the creation of EU-GDPR and the Data Protection Act (2018) UK-GDPR

The UK-GDPR is identical to the EU-GDPR but is an independent UK legislation governed and enforced by the UK data protection agency Information Commissioner's Office (ICO) and does not influence EU authorities.

All UK businesses must be 100% compliant with UK-GDPR or face substantial fines for non-compliance.

© 2023 P4P Compliance Management Limited

Why the need for GDPR?

Image by kues1

People have the right to know and have some control over what personal information a business collects, uses, and shares about them.

With major advancement in technology, easier access to the internet via mobile devices, online shopping and the increased use of social media, Google, Facebook, and LinkedIn etc. has resulted in the enormous increase of consumer personal data being captured, used, shared, and stored by businesses.

© 2023 P4P Compliance Management Limited

What is Personal Data?

As defined in the GDPR Personal Data is a legal term, for “any information relating to an identified or identifiable natural person ‘Data Subject’.

An identifiable person is anyone that can be identified, directly or indirectly, such as:

- An identification number i.e. National Insurance Number.
- One or more factors to their physical, physiological, mental, economic, cultural, or social identity.

Linked / linkable personal data, including:

- Name,
- Email address
- Personal identification number i.e. Passport number

Sensitive data, or special category data, is any data that reveals a subject’s information.

Sensitive/Special category personal data includes:

- Racial or ethnic origin
- Political beliefs
- Religious beliefs
- Sexual orientation

You need a lawful basis in order to process special category data, include:

- If the individual (data subject) has given their explicit consent, or made the data public
- Processing is necessary for the organisation to meet obligations in terms of employment, social security, or social protections as is authorised by UK law
- Processing is being carried out in pursuance of legitimate activities (by a law) by a foundation or not-for-profit organisation
- Protecting data subject interests when the subject is unable or incapable of providing consent
- Substantial public health concerns

Non-Sensitive personal data includes:

- Gender
- Date and place of birth
- Post code

© 2023 P4P Compliance Management Limited

Personally Identifiable Information (PII)

Personal Identifying Information (PII) is any type of data that can be used to help identify someone, from their name, address, phone number, passport information, national Insurance number or credit card information.

Identity theft is a common method of PII violation, as this information can provide criminals unauthorised access to an individual's personal information, including bank accounts details, that can be used for fraudulent purchases directly over the internet.

Privacy and Electronic Communications Regulations 2003 (PECR) is the UK's national implementation of the European ePrivacy Directive. It complements the GDPR's general rules on personal data processing by providing specific rules governing electronic communications.
It is essential for companies to have an PECR / ePrivacy policy so everyone in the organisation adheres to keeping their digital data secure.

There are specific rules on:

- Marketing calls, emails, and texts
- Internet cookies - text files with small pieces of data such as a username and password used to identify your computer while browsing on-line
- Keeping communications secure, including customer location and billing information

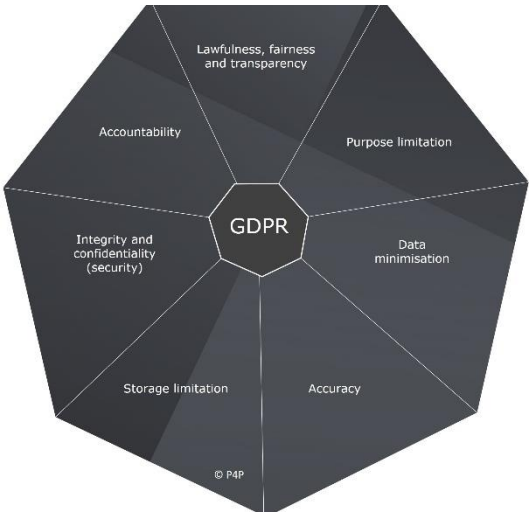
If you send electronic marketing or use cookies on your business website, you must comply with both PECR and the UK-GDPR.

Anyone who breaches PECR can receive a monetary penalty notice imposing a fine of up to £500,000 which can be issued against the organisation or its directors. Or at worse a criminal prosecution, non-criminal enforcement, and audit by The Information Commissioner (ICO).

© 2023 P4P Compliance Management Limited

7 Principles of GDPR

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability



These seven principles set out in Article 5 of the UK-GDPR is essentially the approach an organisations should take when processing personal data.

It requires that personal data be:

1. Processed lawfully, fairly, and transparently
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate and kept up to date where necessary
5. Rectified or erased without delay if it is inaccurate.
6. Stored in a format which enables identification of data subjects for no longer than is necessary
7. Processed in a way to ensure appropriate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage

These principles are the fundamental building block for good data protection practice, and key to complying with the UK-GDPR.

Failure to comply with the principles can lead to substantial fines, for infringements of the basic principles for processing personal data.
A fine of up to £17.5 million, or 4% of an organisations total annual turnover, whichever is higher.

© 2023 P4P Compliance Management Limited

GDPR Roles and Responsibilities

All organisations and companies that work with personal data should appoint a Data Controller or Data Protection Officer. This person(s) is in charge of GDPR compliance, and a single point of contact for employees.

There are tough penalties for those companies and organisations who don't comply with GDPR and can face fines of up to 4% of their annual global revenue or up to £17.5 million, whichever is greater.

© 2023 P4P Compliance Management Limited

Data Controller

The UK-GDPR defines a Data Controller as a person(s) within a business, sole trader, or other legal entity, who determines the purposes, and the way customer and or employee personal data is obtained and processed.

The Data Controller is the manager of personal data and determines who's responsible for GDPR compliance rules, and how data subjects (individuals) can exercise their rights.

The Data Controller decides the purpose for which personal data is required and what personal data is necessary to fulfil that purpose.

The Data Controller is responsible for:

- **Compliance with the data protection principles**
  As described above the Data Controller must comply with the data protection principles.
- **Individuals' rights**
  Ensuring that individuals can exercise their personal data rights, including the rights of access, rectification, erasure, restriction, data portability, objection, and rights in relation to automated decision-making.
- **Security**
  Implementing appropriate technical and organisational measures to ensure the security of personal data.
- **Choosing an appropriate processor**
  Assessing and employing a competent processor to process the personal data in line with the UK-GDPR's requirements.
- **Processor contracts**
  Enter into a binding contract or other legal act with your processor(s), in the instance a controller uses a processor to process personal data on their behalf.
  The contract sets out details of the processing, and that both parties understand and acknowledge their responsibilities and liabilities.

  The contract as specified in Article 28(3), must contain specific compulsory provisions:

  - The subject matter of the processing
  - The duration of the processing
  - The nature and purpose of the processing
  - The type of personal data involved
  - The categories of data subject
  - The controller's obligations and rights

© 2023 P4P Compliance Management Limited

- **Notification of personal data breaches**
  For notifying personal data breaches to the ICO, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. And for notifying affected individuals, if the breach is likely to result in a high risk to their rights and freedoms.
- **Accountability obligations**
  Complying with accountability obligations, such as maintaining records, carrying out data protection impact assessments and appointing a Data Protection Officer.
- **International transfers**
  Complying with the UK-GDPR's restrictions on the transfer of personal data outside of the UK.
- **Co-operation with supervisory authorities**
  Cooperating with supervisory authorities, such as the ICO and assisting them perform their duties.
- **Data protection fee**
  Unless exempt, pay the ICO a data protection fee if you're a business, organisation or sole trader processing personal data.

  There are three tiers of fees set by Parliament to reflect what it believes is appropriate based on the risks posed by the processing of personal data by controllers.

  1. **Micro organisations**
     With a maximum turnover of £632,000 for your financial year or no more than 10 members of staff.

  2. **Small and medium organisations**
     With a maximum turnover of £36 million for your financial year or no more than 250 members of staff.

  3. **Large organisations**
     All controllers as eligible to pay a fee in tier 3 if:
     - They do not meet the criteria for tier 1 or tier 2.
     - Or until they inform ICO otherwise.

  Check if you need to pay the data protection fee
  Or call The ICO helpline **0303 123 1113**

© 2023 P4P Compliance Management Limited

Data Processor

The UK-GDPR defines a Data Processor as a legal or a natural person, agency, public authority, or any other body who processes personal data on behalf of the company's Data Controller.

Data Processors have less ability and freedom over the data they process, however they do have direct legal obligations under the UK-GDPR.

The Data Processor is responsible for:

- **Controller's instructions**
  Only processing personal data on instructions from a controller (unless otherwise required by law).
- **Processor contracts**
  Entering into a binding contract with the controller and complying with the obligations as a processor under the contract.
- **Sub-Processors**
  The Data Processor may engage another processor (a sub-processor) as necessary, with the Data Controller's prior written authorisation.
  When the Data Controller authorises the use of a sub-processor, the Data Processor must have a contract with the sub-processor that contains data protection terms equivalent to those between the Data Processor and the Data Controller.
- **Security**
  Implementing appropriate measures to ensure the security of personal data, including protecting against accidental loss, alteration, unauthorised access, and disclosure or accidental or malicious destruction of such data.
- **Notification of personal data breaches**
  Notifying the Data Controller without delay, so they can contact ICO immediately (no later than 72 hours after having become aware of it) if they become aware of a personal data breach.
  Assist the Data Controller and ICO in complying with its obligations regarding personal data breaches.
- **Notification of potential data protection infringements**
  Notifying the Data Controller without delay of any activities brought to their attention, such as a violation, or an unauthorised act that may lead to a breach of the UK-GDPR laws.
- **Accountability obligations**
  Maintaining records and appointing a Data Protection Officer.
- **International transfers**
  Ensuring that any transfer of personal data outside the UK is authorised by the Data Controller and complies with the UK-GDPR's transfer provisions.
- **Co-operation with supervisory authorities**
  To cooperate with ICO and other supervisory authorities to help them perform their duties.

© 2023 P4P Compliance Management Limited

Data Protection Officer (DPO)

The UK-GDPR requires an organisation to appoint a Data Protection Officer (DPO) if they perform functions of public administration.
Typically these are government departments, Legislative Bodies, Houses of Parliament, The Armed Forces, The National Health Service (NHS) and Registered Charities, and privately owned companies such as schools.

DPOs assist monitor internal compliance, inform and advise on an organisations data protection obligation, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the ICO.

The DPO can be an existing employee or externally appointed, but must be independent, an expert in data protection who reports to the highest management level.

The Data Protection Officer is responsible for:

- Monitoring compliance with the UK-GDPR and other data protection laws, in accordance with the company's data protection policies, awareness-raising, training, and audits.
- Being the company's point of contact for ICO and co-operating with them in the event of a data breach.
- Being the company's point of contact for employees, and other individuals such as contractors for informing and advise them about their obligations to comply with GDPR.
- Managing internal data protection activities and raising awareness of data protection issues, training staff and conducting internal audits

© 2023 P4P Compliance Management Limited

Who needs to comply with the GDPR?

The UK-GDPR applies to 'Data Controllers' and 'Data Processors' within the UK. It also applies to organisations outside the UK that offer goods and or services to individuals in the UK.

Exemptions from UK-GDPR

In some circumstances, the Data Protection Act 2018 (DPA 2018) provides an exemption from particular UK-GDPR provisions.

The UK-GDPR does not apply to the personal data processed:

- By competent authorities for law enforcement purposes
- For the purposes of safeguarding national security or defence
- For purely personal or household activity, with no connection to a professional or commercial activity

There are several different exemptions, including:

- Crime, law and public protection
- Regulation, parliament and the judiciary
- Journalism, research and archiving
- Health, social work, education and child abuse
- Finance, management and negotiations
- References and exams

  Depending on why you process personal data, will determine if you are exempt.
  For more information, see ICO guide to the data protection exemptions

© 2023 P4P Compliance Management Limited

Accountability and Data Governance

The GDPR promotes accountability and governance, which complement the GDPR's transparency requirements.

Organisations must implement effective policies, procedures, and tools like privacy impact assessments and privacy by design to minimise data breach risks and protect personal data.

A key principle is accountability, making companies responsible for demonstrating compliance with the data protection legislation. While the regulation is clear on what needs to be done, many organisations struggle with how to do it.

Data Governance can help strengthen GDPR compliance and provides a framework for managing and defining company policies, business rules, and data assets to deliver the necessary level of data protection and quality.

Data Governance covers any individual or group that has an interest in how data is created, collected, processed, stored, shared, and deleted. Data governance can strengthen compliance by providing a framework to manage policies, rules, and data to deliver necessary protection and quality.

Data Stakeholders who make Data Governance decisions on the lifecycle of company data are accountable for information processes. They decide what people within the organisation can do with data, when and under what circumstances they can do it.

© 2023 P4P Compliance Management Limited

GDPR Breaches and Fines

Personal Data Breach

A personal data breach occurs when an individual's personal data is compromised through an incident that impacts the security of that data.
This incident could be accidental or deliberate and unlawful, leading to the destruction, loss, alteration, unauthorised disclosure, or unauthorised access of the individual's personal information.

Personal Data Breaches include:

- Access to an individual's personal data by an unauthorised person(s)
- Deliberate or accidental action or in-action by a Data Controller or a Data Processor
- Sending personal data to an unintentional or incorrect recipient.
- Personal data being lost or stolen on a computing device such as a laptop or memory stick
- Altering personal data without permission.
- Availability of personal data

In the event of a data breach incident, as a business if you do not manage it in an appropriate and timely manner, it may result in physical, material, or non-material damage to individual (s).

This includes:

- Loss of control over personal data
- Limitation of their rights
- Identity theft, fraud and possible financial loss
- Pseudonymisation of data by replacing information which could be used to identify an individual with false information, such as a value which does not allow the individual to be directly identified
- Damage to reputation

Upon becoming aware of a data breach, you must swiftly contain it and assess its potential impact on affected individuals, including any harm it may cause to their rights and freedoms. You must thoroughly document your response process, in accordance with the GDPR's accountability principle.

The UK-GDPR requires you to inform all impacted individuals directly and as soon as possible about the breach, and its risk impact.
You need to provide them with the name and details of your Data Protection Officer or a single point of contact for advice and support so individuals can protect themselves

Even if you decide against notifying individuals, the ICO must still be informed. They can compel you to notify individuals if the risk is deemed high.

© 2023 P4P Compliance Management Limited

Notifying ICO of a Data Breach

You must report a notifiable data breach to the ICO without unnecessary delay, and not later than 72 hours after becoming aware of it.
If you take longer than this, you must give reasons for the delay.

When reporting a data breach you must provide:

- A description of the personal data breach including, where possible the categories and approximate number of individuals concerned, and the categories and approximate number of personal data records concerned.
- The name and contact details of the Data Protection Officer or a single point of contact point where more information can be obtained
- A description of the likely consequences of the personal data breach,
- A description of the measures taken, or proposed actions to be taken to deal with the personal data breach

  It may be impossible to investigate a data breach fully within the given time period, so the ICO allows you to provide information in phases.

Failing to notify the ICO of a breach when required to do so can result in a fine of up to £8.7 million or 2 per cent of your global turnover.

Reporting a data breach to ICO
https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

© 2023 P4P Compliance Management Limited

Fines and Penalties

One of the major features of the UK-GDPR is the ability for regulators to issue businesses with huge fines or serious penalties for failing to process personal data correctly.

Failing to comply with GDPR businesses face prosecution action by the ICO, who can issue penalties for a data breach including:

- Warnings and reprimands
- Compliance orders
- Bans on processing or data transfers, temporary or permanent
- Administrative fines

Some of these penalties will apply to both Data Controllers and Data Processors and may significantly impact day-to-day business operations.

The ICO determines the level of penalties issued to a company that breaches GDPR by considering:

- The nature, gravity, and duration of the infringement
- The number of people affected and the extent of the damage to them
- Whether the breach was intentional or negligent
- Any previous history of non-compliance
- Any action taken to mitigate the damage
- Whether the Data Controller notified the ICO of the infringement and co-operated

The maximum fine ICO can issue to an organisation is £17.5 million or 4 per cent of their annual global turnover, whichever is greater.

Smaller offences can result in reduced fines up to a maximum fine of £8.7 million or up to two per cent of their annual global income.
The fines are discretionary, not mandatory, and decided by the ICO, on a case-by-case basis.
Money from data breach fines are redirected to the UK HM Treasury, however the ICO is able to retain specified amounts of the funds in response to the Civil Monetary Penalties (CMPs) to cover costs.

Not all GDPR data breaches result in monetary fines, as ICO can decide to take other appropriate actions, such as:

- Issuing warnings and reprimand
- Imposing a temporary or permanent ban on data processing
- Ordering the rectification, restriction, or erasure of data
- Suspending data transfers to third countries

© 2023 P4P Compliance Management Limited

Impact of Non-Compliance

The impact of fines for a breach of data protection regulations can be devastating, however, there are other factors to consider, such as the financial loss you may experience as a result of a data breach.

Businesses may be subject to:

- Private claims for compensation for damages suffered from individuals or consumer protection or legal bodies on behalf of individuals
- Damage to business reputation
- Loss of consumer trust
- Loss of customers, sales and revenue
- Loss of intellectual property if hackers manage to steal designs, strategies, and proposals
- Hidden costs such as legal fees, breach investigation experts, legal fees and hike in business insurance premiums

© 2023 P4P Compliance Management Limited

Benefits of GDPR for Businesses

1. **Competitive Advantage**
   Investing in GDPR compliance and data governance can set you apart from competitors. It shows your commitment to data privacy and security. It also builds trust with customers and employees, making them more loyal.

2. **Time and Cost Savings**
   The GDPR provides time and cost savings by automating and streamlining data management processes. Additionally, it strengthens cybersecurity, safeguarding against potential attacks and mitigating risks of noncompliance, fines, and legal fees.

3. **Auditing of data**
   Conducting an audit of existing data and data management procedures is one of the first steps toward GDPR compliance. This undertaking, though challenging initially, provides businesses with significant long-term advantages. The audit gives organisations a clear overview of the personal information they hold, enabling them to correct inaccuracies, eliminate redundant or obsolete data in physical and digital forms, and retain only high-quality, valuable, relevant data.

4. **Collaboration between teams**
   To comply with GDPR, different teams in a business that often use the same data are encouraged to collaborate. This collaboration requires clear communication, shared responsibility for data security, and coordinated efforts between the teams.

© 2023 P4P Compliance Management Limited

Benefits of GDPR for Consumers

Every consumer leaves a data trail as they go about their daily lives, from the websites they visit to the online transactions they make.

More and more of our personal information is shared with organisations, leading to us consumers becoming increasingly concerned how our personal data is used. Particularly with the increase in cybercrime, and scams.

Under the GDPR consumers can benefit from the following:

1. **Improved consumer rights**
   GDPR gives individuals more control over their personal data, with rights to their personal data, such as access, modification, erasure, restriction of processing, portability, and the right to oppose.

2. **Correct usage and storage of personal data**
   Consumers can be confident that their personal data captured by businesses will only be used for the purposes they have agreed to, giving them faith that their data is being kept and used correctly.

© 2023 P4P Compliance Management Limited

3. **Accuracy of data**
   Businesses need to carry out an audit of existing data and data management processes illustrating exactly what information they hold on individuals.

4. **Right to amend incorrect personal data**
   Consumers can demand an organisation to change or update any of their personal details stored that is inaccurate.

5. **Right to be forgotten**
   Consumers have the right to request deletion or removal of their personal data in certain circumstances, such as when the data is no longer accurate or when an individual withdraws consent for a company to hold their personal information, like unsubscribing from marketing materials.

6. **Right to portability**
   Consumers can demand access and possession to all the personal data an organisation hold on them, in order to transfer it easily to another provider, for example changing banks.

7. **Less marketing spam**
   The GDPR has made it easier for individuals to control what marketing material they receive from companies.
   It requires organisations like banks, insurers, retailers, and others to obtain explicit consent from individuals (data subjects) before sending targeted marketing communications.
   For instance, pre-ticked boxes that automatically sign-up consumers for email marketing are now prohibited and requires consumers to actively opt-in and subscribe.

© 2023 P4P Compliance Management Limited

Conclusion

The GDPR is not about fines, instead it aims to increase transparency and accountability for companies handling personal data, while also empowering individuals with new rights over their information.

The GDPR grants individuals greater control via enforceable rights, such as the right of access, rectification, erasure, and data portability.
It also enables them to make a complaint with regulators and seek effective judicial remedies.

GDPR has provided organisations a single set of rules and a harmonised framework for the protection of personal data.

Ultimately, the GDPR is an opportunity for organisations to strengthen privacy protections in ways that can also generate more business and safeguard sensitive data.

Image Credits
Cover image by DC Studio
Why the need for GDPR by Kues1
7 Principles of GDPR © P4P
GDPR Roles and Responsibilities by Drazen Zigic
Notifying ICO of a Data Breach by Kate Mangostar
Impact of Non-Compliance by Image by Drobotdean
Benefits of GDPR for Consumers by rawpixel.com

Disclaimer

P4P Compliance Management Limited strives to provide the most current and accurate information through diligent research at publication. However, some details may understandably become outdated over time.
This guide is for informational purposes only and does not constitute legal advice. We make no guarantees about the completeness, accuracy, reliability, suitability, or availability of any information, products, services, or related graphics in this article.

All images used in this article are purchased, free stock, or CC0 licenced and accredited to the artist where possible.

© 2023 P4P Compliance Management Limited