Sources of GDPR Information and News

ICO

The UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
www.ico.org.uk

EU GDPR Guidance

European resource to help you to find out how updates to data protection rules will affect you individually, or apply to your business.
https://bit.ly/2Fa05Kl

PYXI for GDPR

UK small business GDPR support, tips and news.
www.pyxi.co.uk
gdpr.team@pyxi.co.uk

Data Subject: An EU resident who is alive. Can also be referred to as a Natural Person.

Child: A Data Subject who requires parental consent.

Personal Data: Data which relate to a living individual who can be identified. Examples include Name, Location Data, Online Identifier.

Sensitive Data: Special categories of information relating to a Data Subject. Examples include race, ethnicity, political beliefs, religious or philosophical beliefs, sexual orientation, biometric data.

Processing: Operations which are performed on personal data, such as collection, recording, structuring, storing, use, retrieval, adaptation. Profiling: Any form of automated processing of personal data to evaluate certain personal aspects relating to a Data Subject. Particularly the analysis or prediction of an individual’s work performance, economic situation, health, personal preferences,. Interests, reliability, behaviour, location or movements.

Consent: Any freely given, specific, informed and unambiguous indication of the Data Subject’s wishes by which they, by a statement or clear affirmative action, signify agreement to the processing of personal data relating to them.

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data Protection Impact Assessment (DPIA): An assessment of the envisaged processing operations on the protection of personal data and the rights and freedoms of Data Subjects.

Subject Access Request (SAR): A request made by a Data Subject to access personal data held by a Data Controller.

Data Protection Officer (DPO): A person with expert knowledge of data protection laws and practices who assists the Data Controller (or Processor) to monitor internal compliance with GDPR. DPOs should be in a position to perform their duties in an independent manner.

1

Acknowledge

GDPR affects every business in the UK as well as not-for-profit groups, informal associations, charities and sole traders.

In short, anyone who processes Personal Data is responsible for complying with the General Data Protection Regulation.

This ensures we all benefit from increased protection of our personal information, and have more control and visibility of what we consent to share, and how it is used by and cared for by those we share our data with.

This means you, as a Data Controller, are accountable for the Personal Data you are processing.

2

Define

What personal data do you store and use in your business?
e.g. contact information, demographic profiles, purchases and service details, contracts, healthcare details, etc.

Whose personal data do you store in your business?
e.g. customers, clients, suppliers, prospects, members, partners, others.

Do you store personal data about people in **High Risk Groups**?
e.g. children, vulnerable adults, etc.

3

Identify

Why and **How** do you use the personal data?
e.g. marketing, customer service, compliance checking, safeguarding, etc.

Where do you store the personal data?
e.g. on computers, laptops, on your website, in the “cloud”, in apps, within software, in spreadsheets, etc.

Who has **Access** to the personal data?
e.g. employees, third-parties, partners, suppliers, regulators, etc.

4

Review

How do you gain and ensure the person’s **Consent**?
e.g. on signup forms, in contracts, verbally, using signatures, etc.

How do you **Secure** and **Protect** the personal data?
e.g. passwords, encryption, backups, etc.

How do you ensure and monitor your **Ongoing Compliance**?
e.g. regular checks and review, external audit, education, staff training, testing, etc.

5

Plan

How will you manage a **Subject Access Request (SAR)**?
e.g. informally, using a planned process, third party assistance, etc.

This includes updating Subject’s data in line with the SAR.

How will you manage a personal **Data Breach**?
e.g. informally, using a planned process, third party assistance, etc.

This includes notifying those affected and putting remedial solutions in place to prevent recurrence.

6

Learn

How will you **Keep Up to Date** with GDPR and other data legislation?
e.g. regularly visit the Information Commissioner’s Office website, attend seminars, read books, subscribe to PYXI’s Weekly Newsletter, etc.

PYXI for GDPR

For more GDPR information, ideas and support for UK Small Businesses
visit **www.pyxi.co.uk**
or email **gdpr.team@pyxi.co.uk**