Lawson-West Solicitors

General Data Protection Regulation (GDPR) and how it applies to your clients and customers

The contents of our GDPR meetups are for general information only. Nothing in our GDPR meetups gives rise to a solicitor/ client relationship. Specialist legal advice should be taken in relation to specific circumstances.

Lawson-West Solicitors

Background

- The new General Data Protection Regulation (GDPR) comes into force in the UK from 25th May 2018.
- GDPR is an update of data law, It replaces all current data protection legislation including the Data Protection Act 1998.
- Non compliance with GDPR is expensive, may result in heavy fines and damage to reputation.
- Fines are up to $20million or up to 4% of annual turnover, whichever is higher.

Lawson-West Solicitors

Who does GDPR apply to?

- Every entity i.e. company, individual or organisation that uses personal data from EU citizens.

- If you or your organisation holds, uses or processes personal data about UK or EU citizens- which includes employees, workers, customers or clients and members of the public then GDPR applies to you.

Lawson-West Solicitors

GDPR and Brexit

- After Brexit the Data Protection Bill will be enacted in the UK to implement the requirements under GDPR.

- Therefore your organisation will still need to comply with GDPR standards after Brexit.

Lawson-West Solicitors

What is data?

- **Personal Data**

  Any information that could identify a living person i.e. name, email, telephone number, address

- **Special Categories of Personal Data**

  Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, data concerning health, sex life and sexual orientation, genetic data or biometric data. This needs more care than personal data because any breach or loss of that data could cause a more significant risk to a person's fundamental rights and freedoms which GDPR is designed to protect.

Lawson-West Solicitors

Grounds for processing data under GDPR

If you want to process personal data about an individual you must have a legal basis for doing so. GDPR states six legal grounds which permit personal data processing are:

1. Consent
2. Performance of contract
3. Compliance with a legal obligation
4. Vital interest of the data subject
5. Public interest
6. The legitimate interests of the data controller

Lawson-West Solicitors

Principles governing the processing of personal data under GDPR

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity & confidentiality

Lawson-West Solicitors

Rights of Data Subjects

Increased rights for Data Subjects under GDPR including:

- The right to information- for all information on them to be provided including who its being shared with.
- The right to erasure (to be forgotten)- that all data on a person is deleted.

Lawson-West Solicitors

Rights of Data Subject Continued

- The right to withdraw consent- it must be easy for a data subject to quickly withdraw consent provided previously.
- The right to data portability- individuals can obtain and reuse their personal data for own purposes across different services.
- The right to object – to forms of processing or direct marketing.

Lawson-West Solicitors

What to do next

Lawson-West Solicitors

1. Carry out an assessment or audit on your data

- What data do you hold?
- Where is data held and what is it used for?
- Can you identify potential security breaches?
- Do you have a record of any third parties you share data with, has the individual consented to this?
- Is data securely kept whether online or in the office?
- How long is data kept for?
- Can you find the data in the event of a request from a data subject and can you delete it?
- Do you have a process for reporting any breach to an individual within 72 hours of its occurrence? A data breach is classed as the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Lawson-West Solicitors

2. Identify what is your legal basis for collecting data?

- Processing activities that fall under performance of a contract, legal obligation, vital interests and public task may be fairly straight-forward to identify. The key for many will be assessing whether **Consent** or **Legitimate Interests** will be most appropriate for processing of personal information.

Lawson-West Solicitors

Consent

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

Lawson-West Solicitors

What does this mean?

- Consent requires a positive opt-in. Not permitted to use pre-ticked boxes or any other method of consent by default.
- Consent mustn't be a pre-condition and should not be bundled in with Terms & Conditions.
- It must be clear who will use the data and how.
- Keep a record of what is given, when and how.
- You must have this detail for all records stored including those prior to May 2018.
- If you do not have this and you are relying on consent you will need to re-permission all persons in accordance with GDPR.

Lawson-West Solicitors

Consent is one lawful basis for processing, but there are five others. Consent won't always be the easiest or most appropriate.

Lawson-West Solicitors

Legitimate Interest

"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".

Lawson-West Solicitors

What does this mean?

- There must be a **relevant and appropriate relationship** between you and an individual for example where an individual is an existing client or expressed an interest in your products and services and that there is a **reasonable expectation** their data will be processed.
- You need to show you have **balanced your interests** with the interests and rights of the individuals affected by your proposed processing activity and these interests do not override your legitimate interest. This assessment should be documented.
- You will need **to inform individuals** that you are processing their personal information under this condition (i.e. via your Privacy Notice).
- You will need to be able to **uphold the individual's right to object** to such processing.

Lawson-West Solicitors

Using Legitimate Interests when marketing

- GDPR gives examples of processing that could be necessary for the legitimate interests of a data controller. One of these include processing for direct marketing purposes.
- Legitimate Interests might be a tempting option to justify processing an individual's data for marketers but beware of Privacy and Electronic Communications Regulations 2003 (PECR), PECR gives marketers specific rules concerning sending marketing emails, text messages or conducting telemarketing calls.
- Under PECR In some circumstances you will have to obtain Consent and this consent must meet GDPR standards.

Lawson-West Solicitors

When do you need Consent?

- Email/Text: PECR stipulates that you must not send marketing emails or texts to individuals without specific Consent (unless an exemption applies).

Lawson-West Solicitors

When are you NOT required to have Consent?

- Email/Text: There is an exemption within PECR, known as the “soft opt-in”, whereby you can send emails/texts without Consent as long as the following conditions are met:
- You have obtained the data in the course of a sale (or negotiations of a sale) of a product or service
- You are only marketing your own similar products and services
- You provided an easy opportunity to refuse or opt-out of the marketing, when you first collected the data and in every subsequent communication.
- This means you may be able to email or text your own customers without Consent, but this will not apply to prospective customers or bought-in lists.

Lawson-West Solicitors

3. Review Your Privacy Notice

A Privacy Notice describes what, how and why personal data are collected and used. Organisations will be required to provide individuals with extensive information about the processing of their personal data.

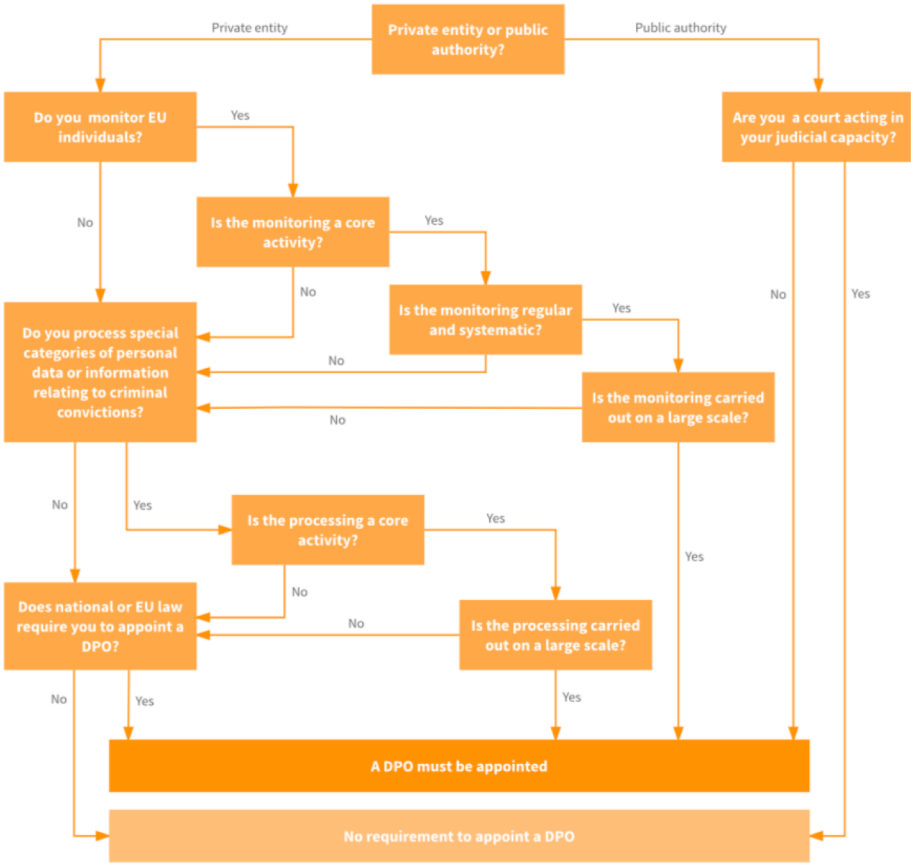
GDPR requires the information in your privacy notice to be concise, clear and easy to understand.

In summary the following should be covered by a privacy notice:

- Your basis for processing data-how you are going to use the personal data and why?
- Data retention periods- how long will you keep the personal data on record for?
- The individual's right to request access to, deletion of or correction of, their personal data or complain to a supervisory authority i.e. the ICO.

Lawson-West Solicitors

4. Do you need to appoint a Data Protection Officer?



Lawson-West Solicitors

5. Train your staff

Training programmes should be put into place for staff handling data. These are some of the things to cover:

- Do staff understand their responsibilities under GDPR?
- Reporting potential breaches to the individual(within 72 hours of awareness under GDPR).
- Is there a central point of contact such as Data Protection Officer or someone else to which enquiries can be directed to?
- Are your staff able to handle the rights of individuals promptly?

Lawson-West Solicitors

Positive Points From GDPR

- Organisations are forced to send more relevant communications.
- Opportunity to reconnect with previous contacts.
- Happier more targeted audience.

Lawson-West Solicitors