VinciWorks

General Data Protection Regulation Checklist

Making sure your business is GDPR compliant

Article 5 of GDPR requires demonstrable compliance with the new data protection regulations. With GDPR now in force, ensuring your staff are aware of your organisation's data protection policies is now more important than ever. Use this checklist to help you establish whether you have everything in place to be compliant with GDPR.

GDPR Checklist

☐ Are you familiar with GDPR?

Staff who regularly process data should be familiar with GDPR and the changes in data protection under GDPR. You can download a guide to GDPR here.

☐ Do you know how many personal records you process per year?

This is important information to be aware of. Companies that process over 5,000 personal records per year are required to appoint a Data Protection Officer (DPO).

☐ Do you have a process for data portability?

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. You must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data. The information must be provided free of charge.

☐ Do have a process for data erasure?

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing. Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this threshold is not present.

☐ Do you inform individuals about the data you process?

Being transparent and providing accessible information to individuals about how you will use their personal data is a key element of GDPR. The most common way to provide this information is in a privacy notice. To cover all these elements you will need to consider the following issues when planning a privacy notice: What information is being collected? Who is collecting it? How is it collected? Why is it being collected? How will it be used? Who will it be shared with? What will be the effect of this on the individuals concerned? Is the intended use likely to cause individuals to object or complain?

☐ Do you have justification for transferring data outside of the EU?

GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of GDPR.

☐ Have you appointed a Data Protection Officer?

Organisations are required to employ a DPO if they fit into at least one of these categories: process over 5,000 personal records per year, employ 250 staff members or more, or are in the public sector. Existing DPOs will have their roles strengthened and will report to the highest levels of management.

☐ Do you have a Data Protection Policy in place?

We strongly recommend having an up-to-date Data Protection Policy in place. The document should detail who the DPO is, the procedures for processing data and the responsibilities of each department when processing data. All staff should be aware of the policy. You can download a Data Protection Policy template that can be edited to suit your business here.

☐ Do you have a Privacy Policy in place that can be easily found on your company website?

A privacy policy explains what information is collected, how the information is used and why it is being collected. The policy should be made available on the company website.

☐ When processing data, are the following principles met?

- *The processing is lawful, fair and transparent*
- *Are you transparent about what the personal data is being used for?*
- *The data is collected for a specific purpose*
- *The data is necessary for its purpose*
- *The data must be accurate and kept up to date*
- *Data is not kept for longer than necessary*
- *The data is kept safe and secure*

☐ Is the data your organisation processes considered sensitive information?

Organisations that process data containing sensitive information about an individual must also appoint a DPO. The following is considered sensitive data:

- *Racial or ethnic origin*
- *Political opinions*
- *Information about their physical or mental health*
- *Religious beliefs*
- *Information about their sexual life*
- *Information about any existing or past criminal convictions against them*

☐ Do you have sufficient data protection training in place?

We recommend that all employees whose role requires them to process or store personal data undertake data protection training. The training should provide the latest information in data protection policy and law, as well as help staff understand how data protection laws affect their role within the organisation.

VinciWorks is a leading global provider of online compliance training. With over 80,000 users across 70 countries, VinciWorks has established itself as the definitive authority in compliance learning.

To learn more about VinciWorks' latest course on data protection visit www.vinciworks.com/dataprotection