GDPR Compliance Checklist

O'Brien Media
creativity with style

Since every business is different and the GDPR takes a risk-based approach to data protection, companies should work to assess their own data collection and storage practices and seek their own legal advice to ensure that their business practices comply with the GDPR. In determining your next steps, here are some of the questions you should consider.

Disclaimer

This legal information is different from legal advice, where a solicitor or properly qualified person applies the law to your specific circumstances, so we insist that you consult a solicitor if you'd like advice on your interpretation of this information or its accuracy. In a nutshell, you may not rely on this paper as legal advice, nor as a recommendation of any particular legal understanding.

The Assessment

What personal data do we collect/store?

Have we obtained it fairly? Do we have the necessary consents required and were the data subjects informed of the specific purpose for which we'll use their data? Were we clear and unambiguous about that purpose and were they informed of their right to withdraw consent at any time?

Are we ensuring we aren't holding it for any longer than is necessary and keeping it up-to-date?

Are we keeping it safe and secure using a level of security appropriate to the risk? For example, will encryption or pseudonymisation be required to protect the personal data we hold? Are we limiting access to ensure it is only being used for its intended purpose?

Are we collecting or processing any special categories of personal data, such as 'Sensitive Personal Data', children's data, biometric or genetic data etc. and if so, are we meeting the standards to collect, process and store it?

Are we transferring the personal data outside the EU and if so, do we have adequate protections in place?

The GDPR Project Plan

Have we put a project plan together to ensure compliance by the May 2018 deadline?

Have we secured buy-in at executive level to ensure we have the required resources and budget on hand to move the project forward?

Do we require a Data Privacy Impact Assessment?

Do we need to hire a Data Privacy Officer?

Are we implementing a policy of 'Data Protection by Design and Default' to ensure we're systematically considering the potential impact that a project or initiative might have on the privacy of individuals?

Have we considered how we handle employee data in our plan?

The Procedures and Controls

Are our Security team informed to ensure they're aware of their obligations under the GDPR and do they have sufficient resources to implement any required changes or new processes?

Do we have procedures in place to handle requests from data subjects to modify, delete or access their personal data? Do these procedures comply the new rules under the GDPR?

Do we have security notification procedures in place to ensure we meet our enhanced reporting obligations under the GDPR in case of a data breach in a timely manner?

Are our staff trained in all areas of EU data privacy to ensure they handle data in a compliant manner?

Do we review and audit the data we hold on a regular basis?

The Documentation

Do we have a Privacy Policy in place and if so, do we need to update it to comply with the GDPR?

Do we have a defined policy on retention periods for all items of personal data, from customer, prospect and vendor data to employee data? Is it compliant with the GDPR?

Are our internal procedures adequately documented?

If we're a data processor, have we updated our contracts with the relevant controllers to ensure they include the mandatory provisions set out in Art. 28 of the GDPR?

In cases where our third party vendors are processing personal data on our behalf, have we ensured our contracts with them have been updated to include those same processor requirements under the GDPR?