Client Alert

HANSUKE

GDPR: Precisely a year to compliance

Contact

Safdar Mirza
Information Security & Data Privacy Specialist
safdarmirza@hansuke.co.uk

Ahmed Nawab
IS Specialist
ahmednawab@hansuke.co.uk

Tel: +44 (0) 203 865 0625

Background

The GDPR comes into force precisely a year from today and will supersede the UK Data Protection Act 1998 ("DPA"). The regulation was adopted on 27 April 2016, and will come into full force from 25 May 2018 after a two-year preparatory transition period. The primary objective of the regulation is to give individuals back control of their personal data, for example, by requesting details of information held by organisations, exercising the right of erasure (i.e. right to be forgotten) and applying for their data to be ported to a different service provider.

Non-compliance with the GDPR will result in penalties of up to €20m of up to 4% of annual global turnover, whichever is greater.

Who does it apply to?

The GDPR applies to organisations operating within the EU, in addition to organisations outside the EU that offer goods or services to individuals in the EU. In other words, all organisations that collect and process personal data of EU citizens, regardless of their physical location, must comply with the GDPR. This applies to both data controllers (organisations that collect data from EU residents) as well as data processors (organisations that process data on behalf of data controllers e.g. cloud service providers).

If your organisation is currently subject to the DPA, it is likely that it will also be subject to the GDPR. The UK's decision to leave the EU will not affect the commencement of the GDPR.

What is expected of me?

Under the GDPR, organisations must ensure personal data are:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Are you prepared?

- Do you know your legal basis for processing data, and have you documented this?
- Do you understand where personal data resides and has this been documented within a data inventory?
- Do you understand the complete data lifecycle of the personal data you hold, from attainment, consent and to disposal, and have you documented this?
- Are you able to evidence you have taken sufficient steps to implement technical and organisational controls to protect personal data e.g. encryption, pseudonymisation, ability to restore availability and access to personal data?
- Do you have procedures in place to report a data breach within 72 hours, and respond to a Subject Access Request ("SAR") within 30 days?
- Do you have procedures in place to facilitate data portability and implement the right to be forgotten?
- Where appropriate, have you appointed a Data Protection Officer ("DPO")?
- Do your contracts with data processors comply with the GDPR?

How Hansuke can help

The expert team at Hansuke incorporates a deep knowledge of the issues that affect the Financial Institutions from over 100 years of cumulative experience. Our team consists of a unique blend of former Regulatory, Legal Firm and "big-4" accountancy personnel who will be able to assist you in with the end-to-end activities that will help you to demonstrate compliance with the GDPR. We would be pleased to have a no-obligation discussion.

About Hansuke

Hansuke is an independent specialist financial services consultancy, providing truly independent advice. We are fully committed to delivering the right advice and solutions. This means that you get the optimal fit for your needs. We have assembled the right blend of expertise: spanning regulatory, information security, information systems and commercial financial expertise.