Kennedys

GDPR - a 10 step launch checklist

The General Data Protection Regulation (GDPR) came into force on 25 May 2018.

The new regulations apply when personal data of EU residents is processed (collected, stored or otherwise used) regardless of where the processing takes place. The UK's Data Protection Bill 2017 brings the data protection law in the UK in line with the GDPR and therefore these changes will continue to apply in the UK post-Brexit.

We have set out a checklist of the key compliance issues for insurers to consider now that the new provisions are in force.

1. Determine what data you hold

Individuals, organisations, and companies that are either 'controllers' or 'processors' of personal data are covered by the GDPR. Accordingly, for insurers, it is critical to work out what personal data (of individuals as opposed to companies) they hold. The GDPR definition of personal data is wider than the current definition in the Data Protection Act 1998.

Essentially, personal data will include any information relating to an identifiable person. This may include their name, an identification number, geo-location data, or mobile device IDs. Where data is anonymised (i.e. an individual cannot be identified from it) it is outside the scope of the GDPR.

2. Determine if you are a data controller or data processor

It is important that you properly understand the basis upon which you are utilising personal data, as the extent of GDPR depends upon the scope of your role:

Data controller?

If you actively collect, record, store, distribute, or erase data and exercise overall control over how and why personal data is processed, then you are a data controller. Insurers are almost certain to be data controllers as there is a necessity to collate personal information for the purpose of underwriting risks, or processing claims. If you are a data controller, there is an obligation to manage your data processors and ensure that there is adequate security in place.

Data processor?

If you process data on behalf of a data controller – for example by storing, organising or transmitting data on someone else's behalf - then you are a data processor. Data processors' obligations have been ramped up by the GDPR and now share some duties with data controllers, particularly in relation to accountability, ensuring appropriate security is in place and responding to rights of access requests by data subjects. Whilst some duties (particularly the legal right to process data) remain vested in the data controller, there are obligations on the data processor to notify any data breaches to the data controller, and failure to do so may result in sanctions.

For insurers, it is important to ensure that data processors who are processing data on their behalf are aware of their obligations and, if necessary, contracts should be amended to reflect these obligations.

3. Do you have a lawful basis to process the data?

There are six lawful bases which provide data controllers with a right to process data:

- ☐ The individual has given clear consent (see below).
- ☐ Processing is necessary to perform a contract with the data subject.
- ☐ Processing is necessary to comply with the law.
- ☐ Processing is necessary to protect someone's life.
- ☐ Processing is necessary to perform a task in the public interest or exercise of an official function, and has a clear basis in law.
- ☐ Processing is necessary for the data subject's legitimate interests or those of a third party, unless there is a good reason to protect that data subject's personal data.

4. Do you have consent?

The issues surrounding consent are a key consideration in the GDPR. Data controllers have a greater responsibility to demonstrate data subjects' consent, where that is the legal basis upon which they rely.

Data controllers must make requests for consent clear and accessible, and be able to demonstrate that the data subject's consent was freely given. Consent must be as easy to withdraw as it is to give.

For insurers, the implication is that where personal details are being used (most particularly in personal lines of insurance), explicit consent will be required. The GDPR states that existing consent which falls in line with the GDPR requirements will not need to be refreshed post GDPR. However, insurers will need to be confident that consent requests already meet the GDPR standard and that consents are properly documented. If not, fresh consent will need to be sought in a clear and well documented way – or processing will need to stop.

5. Have you completed an information audit?

A principle of accountability is built into the GDPR. This means that data controllers are responsible for the data they hold and must be able to demonstrate appropriate systems are in place. An audit on both the systems in place and information/data should be carried out in order to determine what further procedures are required.

The GDPR also requires data controllers to conduct "Privacy Impact Assessments" where privacy breach risks are high and where there is a large scale processing of sensitive information. This is a high burden, and will be relevant for most insurers given the type of information they hold.

6. Has a Data Protection Officer (DPO) been nominated?

The GDPR obliges data processors and data controllers to appoint a DPO where:

- ☐ They are a public body
- ☐ They monitor data on a large scale
- ☐ The core activities involve large scale processing of personal data.

Most insurers will fit this criteria. It is important to appreciate that the DPO should be a separate role to the legal department and report directly to the board.

7. Is there a clear breach notification strategy in place?

A new key requirement of the GDPR is that data controllers are obliged to report the vast majority of security breaches to the relevant supervisory authority "without undue delay, and where feasible, not later than 72 hours" after they first become aware of the issue. Data processors must notify the data controller of any breaches without undue delay after becoming aware of it.

It is therefore vital that systems are in place to ensure that breaches of personal data are identified and acted upon and, where appropriate, notified to the Information Commissioner's Office (ICO) and the data subjects themselves. Failure to do so may result in severe sanctions levied against the organisation. Insurers tend to be multinational organisations with complex team and management structures, but it is essential that every individual in every team understands their GDPR obligations.

8. Ready to comply with new rights of access?

There is a new suite of rights available to data subjects. These include a right to rectification of data, restrict processing and - of most significant impact - a right to erasure.

Insurers will need to be alert to requests by insureds for amendment, deletion and data transfer, and to have a clear, accessible and uniform system throughout the business to ensure compliance can be achieved.

9. Is the data readily portable?

Together with the new rights of access, the GDPR introduces a new right of data portability. This means that, on request, a data controller must provide the data subject with a copy of his or her personal data which was provided by him or her to the data controller (not data which has been generated by the data controller itself) in a 'structured, commonly used and readable format'. Additionally, the data controller must not hinder the data subject's transmission of personal data to a new data controller.

This will have a huge impact on the insurance industry, as there are likely to be requests from insureds (possibly combined with a request for erasure), particularly upon the expiration of policies. It is also essential for the data to be in an accessible format, which can be recognised by another insurer.

10. Have staff been trained?

It is crucial that staff at all levels are alert to the specific areas of GDPR that they may need to consider and the stringent reporting requirements. Training targeted at the specific risks of individual lines of the business is likely to be more effective, as well as embedding data protection in the organisational culture on a more general basis.

Contact

For further information on this subject, please contact:

Tom Pelham
Partner
t +44 161 829 7453
tom.pelham@kennedyslaw.com

Oliver Dent
Solicitor
t +44 161 829 7462
oliver.dent@kennedyslaw.com

To find out more about our services and expertise, and key contacts, go to: **kennedyslaw.com**