DAC beachcroft

The European General Data Protection Regulation

A guide for the insurance industry

IMPORTANT NOTE: This guide is based on the politically agreed compromise text agreed by the European Commission, EU Parliament and the Council of the EU on 15 December 2015 following the final trilogue meeting. The GDPR text still requires formal validation and may be subject to change although we do not expect it to change substantially. This guide is not exhaustive. It is provided solely for general information purposes and should not be relied upon as legal advice. No liability is accepted for errors of fact or opinion this guide may contain. Professional advice should always be obtained before applying the information to particular circumstances. The copyright in this guide is retained by DAC Beachcroft.

Contents

> Data protection will need to be on the boardroom agenda

Rhiannon Webster
Partner, Insurance Advisory
T: +44 (0) 20 7894 6577
E: rwebster@dacbeachcroft.com

This is a milestone moment in the world of data protection law. On 15 December 2015, after 3 years of detailed discussions, political agreement was reached between the European Commission, EU Parliament and the Council of the EU on the compromise text of the General Data Protection Regulation. The GDPR will replace the Data Protection Directive 95/46/EC and therefore the Data Protection Act 1998 in the UK. The GDPR will be formally adopted by the EU Parliament and the Council of the EU in the coming weeks when it is published in the Official Journal of the European Union. Twenty days later, the GDPR will be in force. It will not take effect for a further two years. We anticipate that the GDPR will take effect some time during the first half of 2018.

It is, however, early days. We await further guidance and local legislation where derogations to the GDPR are permitted. We will keep you updated as the landscape evolves.

This guide has been written to provide the insurance industry with an overview of the impact we expect the GDPR to have. We have looked at each of the main provisions and compared them against current law and best practice guidance from the Information Commissioner's Office. We have then considered the impact that these key changes might have on the insurance industry and advised on the practical steps that can be taken now in order start the process of ensuring GDPR compliance before the two year implementation period comes to an end.

HOME

For ease of reference, the impact of each change has been coded as follows:

a positive change for the insurance industry which should ease the compliance burden

little or no change or a change with little or no effect

a negative change for the insurance industry which may restrict processing activities and/or create an additional compliance burden

Much of the GDPR will be familiar territory, with the compromise text supplementing and enhancing those rights and obligations which are already present in the Data Protection Act and associated guidance. However, the GDPR does make the obligations on companies processing personal data more prescriptive and the rights of data subjects clearer and easier to enforce.

The insurance industry will need a greater command over the data it holds, why it is held and how long it is held for. This will require a seismic change of attitude for many companies. Fines, which can now be as much as 4% of annual worldwide turnover, will mean that data protection will need to be on the boardroom agenda. It's time for the insurance industry to get its data (ware)house in order.

> "It's time for the insurance industry to get its data (ware)house in order"

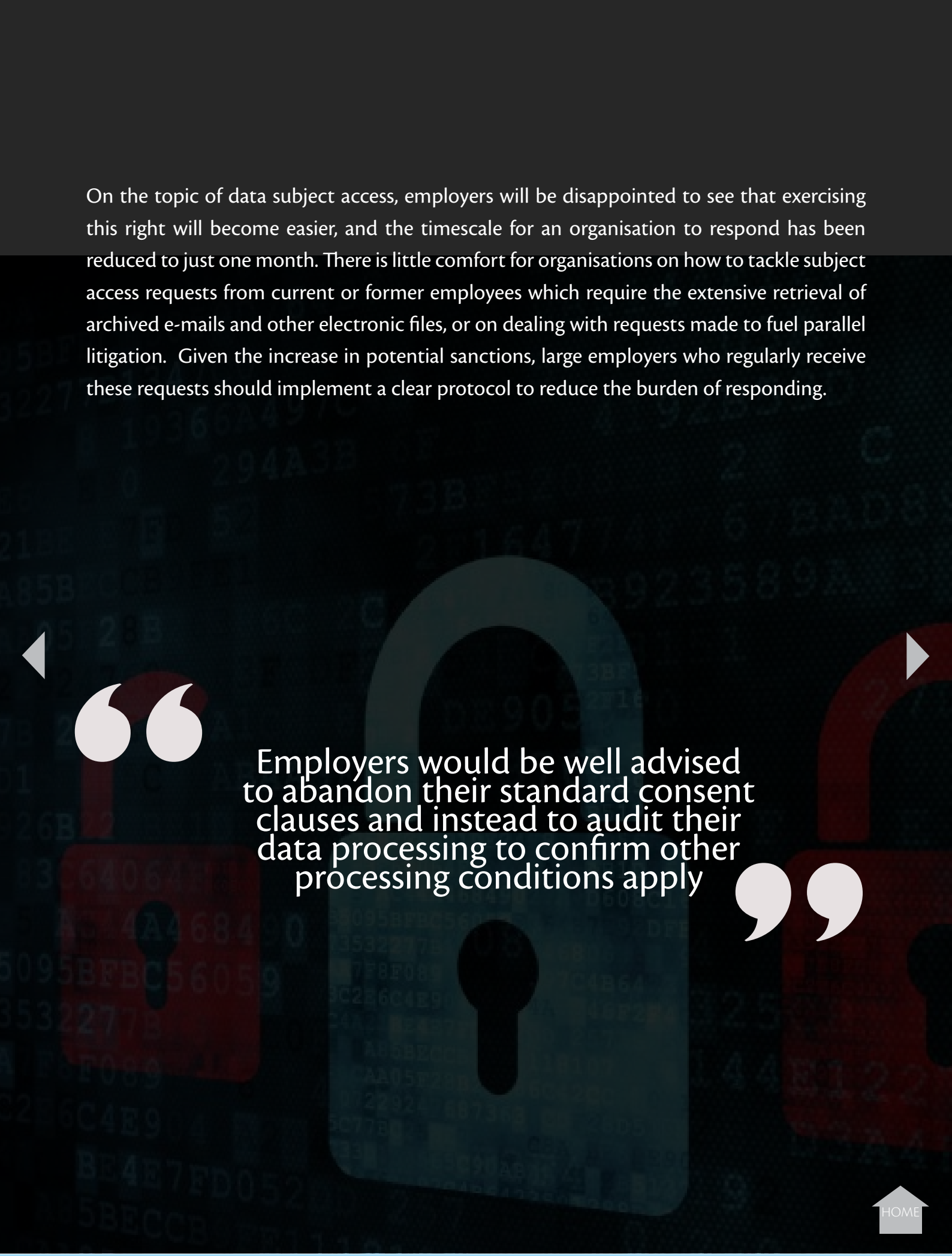
Khurram Shamsee
Partner, Employment
T: +44(0)20 7894 6566
E: kshamsee@dacbeachcroft.com

The GDPR has particular challenges for insurers in their capacity as employers, although the impact of GDPR on the processing of employee personal data will perhaps be felt less acutely than in relation to customer or consumer personal data. Indeed, the GDPR may well mark the beginning of a sharp divergence in how organisations process these different categories of personal data.

A key consideration for all employers is the continued reliance upon consent to legitimise the processing of the ordinary and sensitive personal data of its employees. For a number of years, doubt has been cast on whether the employee/employer relationship is compatible with the requirement that consent is freely given, not least as it has become common practice for employers to include blanket consent provisions in their standard employment contracts (so that the employee has no real choice in the matter). As such, with the encouragement of the ICO, in recent years there has been a move away from employers relying upon consent to instead ensuring that it can satisfy one of the other conditions provided for the processing of ordinary or sensitive personal data. The GDPR reinforces this principle, and it is difficult to see how the more stringent requirements for securing consent will be workable in the employment context. Employers would therefore be well advised to abandon their standard consent clauses and instead to audit their data processing to confirm other processing conditions apply. Employee privacy notices will also need to be updated to cover the information prescribed by the GDPR, along with any separate notice provided to job applicants at the recruitment stage.

HOME

On the topic of data subject access, employers will be disappointed to see that exercising this right will become easier, and the timescale for an organisation to respond has been reduced to just one month. There is little comfort for organisations on how to tackle subject access requests from current or former employees which require the extensive retrieval of archived e-mails and other electronic files, or on dealing with requests made to fuel parallel litigation. Given the increase in potential sanctions, large employers who regularly receive these requests should implement a clear protocol to reduce the burden of responding.



> Employers would be well advised to abandon their standard consent clauses and instead to audit their data processing to confirm other processing conditions apply

Hans Allnutt
Partner, Global
T: +44(0)20 7894 6925
E: hallnutt@dacbeachcroft.com

> The GDPR is the key legal change that European cyber risk insurers have been waiting for

The GDPR is the key legal change that European cyber risk insurers have been waiting for. Cyber insurance provides indemnities for a variety of first party losses and third party liabilities arising out of cyber incidents. In particular, these policies indemnify the costs and expenses incurred by policy holders in the aftermath of data breaches. Such costs are a familiar feature in the US, sometimes running into millions of dollars. This is because it is typical for US companies suffering data breaches to be legally obliged to notify regulators and affected data subjects.

For most companies that suffer data breaches or cyber-attacks in the EU, there is no such requirement to notify either regulators or data subjects. Therefore, data breaches often go unreported with companies facing limited financial and reputation exposure as long as the breach is not made public.

HOME

Recent guidance and a greater sense of corporate responsibility has increased the number of breaches that are reported in the UK, but the GDPR will bring in compulsory notification obligations for all companies which suffer data breaches. The prospect of fines for non-compliance of up to 4% of annual worldwide turnover or €20m, and a 72-hour regulatory notification requirement, are forcing companies to consider what they would do in the event of a significant breach.

- How will we independently investigate a cyber-attack or incident?
- Who can we go to for legal advice at short notice?
- What do we need to know in order to inform our regulators?
- How do we contact data subjects who are no longer customers?
- What is our media strategy?
- How are we going to respond to claims for compensation?

Dedicated cyber and data breach insurance policies are designed to provide financial assistance to companies in order to deal with the many issues following a data breach including those above. Some policies provide response teams which coordinate the legal, forensic and other expert advice required to respond to incidents (often calling upon the services of DAC Beachcroft's cyber and data risk team). A number of high profile data breaches have highlighted the benefits of having such services on hand. With the GDPR now looming, demand for cyber and data breach insurance policies is set to grow.

"With the GDPR now looming, demand for cyber and data breach insurance policies is set to grow"

Journey so far

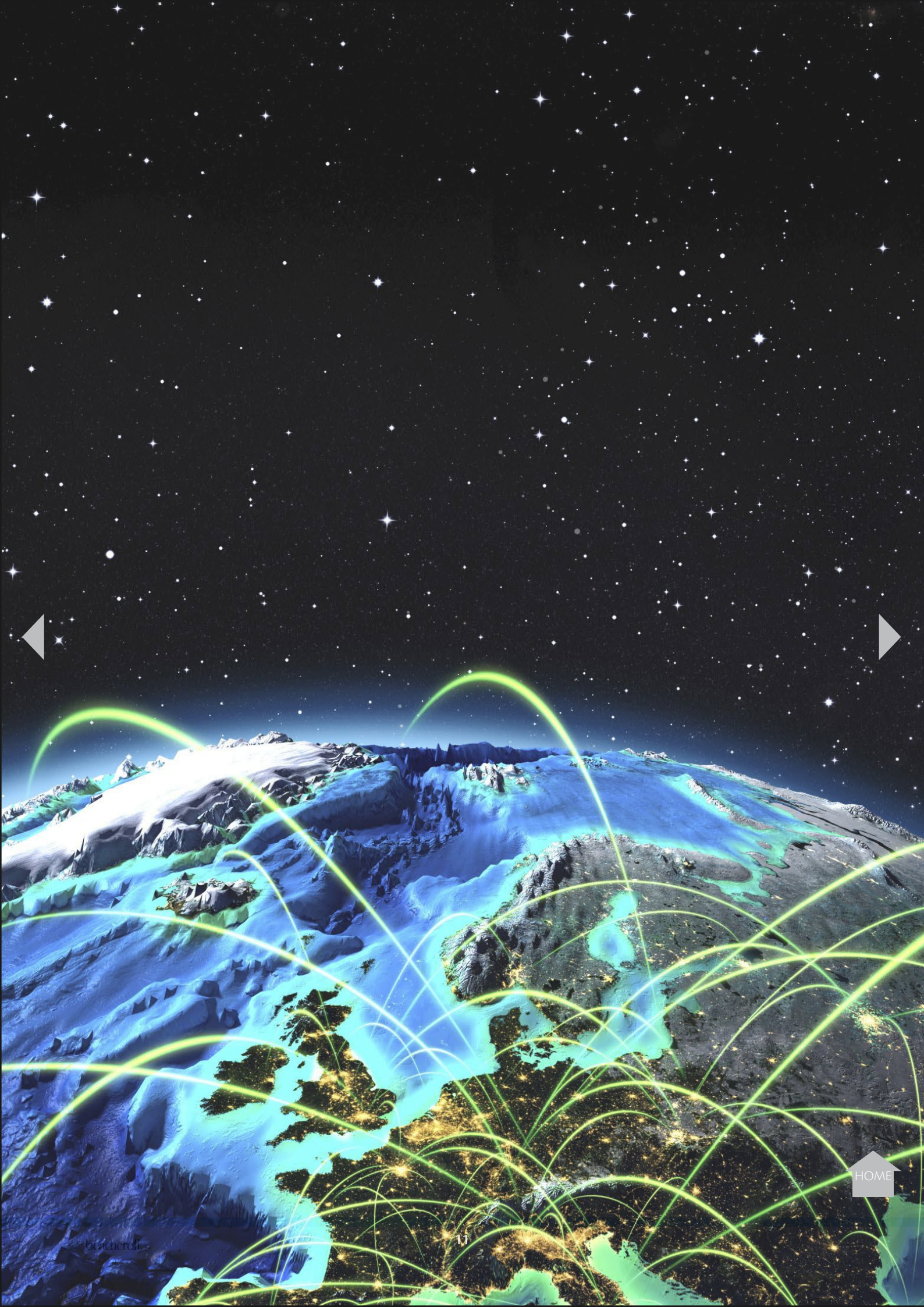
Date	Event	Details
24 October 1995	EU Data Protection Directive agreed	Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (**Directive**)
13 December 1995	Directive entered into force	Publication date in the Official Journal + 20 days
16 July 1998	Data Protection Act 1998	The Data Protection Act 1998 (**DPA**) came into force in the UK implementing the Directive
January 2012	Reform proposed	The European Commission proposed a comprehensive reform of data protection rules within the EU, including a new draft data protection regulation, which would become the GDPR
May 2012 – May 2015	Negotiations	Negotiations between the European Commission, EU Parliament (including its Civil Liberties Justice and Home Affairs Committee or **LIBE Committee**) and the Council of the EU and national parliaments on what the GDPR should include
June – December 2015	Trilogue discussions	Trilogue discussions between the European Commission, EU Parliament and Council of the EU to agree a final text of the GDPR
15 December 2015	Informal political agreement on consolidated text of GDPR	Informal political agreement on final text of the GDPR following the final trilogue discussions
17 December 2015	LIBE Committee approval	The EU Parliament's LIBE Committee approved the politically agreed text

HOME

Journey to come

Estimated Date	Development	Action
Today	Journey to compliance begins	Organisations to begin implementing internal compliance programmes
February 2016	Dutch Presidency of the Council of the EU to determine the strategy and timelines for approval	
February or March 2016	Council of the EU approval to be formalised at a Council meeting in February or if further discussions on the text are required, approval will be formalised at the Justice and Home Affairs Council Meeting in March	
March 2016	EU Parliament's plenary vote to approve the agreed text. Note that the EU Parliament is not formally bound by the LIBE Committee's approval. However, dissent is highly unlikely	
April / May 2016	A committee of experts will consolidate and finalise the GDPR text. No substantial changes can be made to the politically agreed text of 15 December 2015.	
May / June 2016	Translation of the finalised GDPR text into each of the EU's official languages	
June / July 2016	Publication of the finalised GDPR in the Official Journal	
Publication date + 20 days 2016	GDPR comes into force 20 days after its publication in the Official Journal	Organisations now have a two year implementation period to ensure compliance
2016 / 2017	Guidance expected from the European Data Protection Board and national supervisory authorities	
1 year + 1 day prior to GDPR applying	Key compliance date for insurers and brokers	Last date for insurers and brokers to implement new privacy notices into annual insurance policies
July 2018	GDPR to apply (2 years after the date the GDPR comes into force)	Organisations must be operating in full compliance with the GDPR

HOME


HOME

Summary of key changes

Wider Scope

- Data processors now have direct obligations and liabilities
- Expanded territorial scope to govern companies targeting goods and services at EU citizens

New Data Subject Rights

- Right of data portability
- Enhanced right of erasure
- Right to object to profiling

Enforcement

- Fines for the most serious breaches of up to 4% of worldwide turnover or €20,000,000, whichever is higher
- Data subject has right to compensation from a data controller or data processor
- "One stop shop" introduced but significantly watered down from original proposals. Detailed regime with lead authorities and concerned authorities working together

Fair processing notices

Specific and comprehensive requirements for content and format of privacy notices including specifying processing conditions and retention periods

Consent

Higher threshold for consent meaning there will only be limited circumstances when it may be relied upon

Accountability

- New principle of accountability
- Certain processing activities will require a privacy impact assessment in advance
- All new systems should be designed in accordance with privacy by design and privacy by default

Security

- Data subjects to be notified where there is a high risk to rights and freedoms
- Breaches to be notified within 72 hours where feasible
- Pseudonymised data formally recognised as a security protection

Data protection officers

- New requirement to appoint a DPO in certain circumstances
- DPO must be independent and must not be instructed on how to carry out his/her role
- Must report directly to the highest level of management

Best of the rest

- International transfer mechanisms largely unchanged save for formal recognition of binding corporate rules
- European Data Protection Board to replace Working Party 29 with remit for guidance and consistent application of the GDPR
- New concept of data privacy seals

Scope

Definitions and Data Processors

Current position under the DPA and ICO Guidance

The DPA applies to the processing of personal data. Personal data is defined as data from which you can identify a living individual.

Under the DPA, only data controllers have direct obligations in relation to personal data (although ICO guidance widened the scope of what companies would be considered data controllers). Data controllers are defined as a person who determines the purpose and the manner of the processing of personal data. Data controllers are differentiated from data processors who act on the instructions of the data controllers and to whom no obligations under the DPA apply. Data controllers are obliged to put contracts in place with their data processors which oblige the data processors to have adequate security in place and to act only on the instructions of the data controller.

Position under the GDPR

The definition of personal data has been slightly broadened to "any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person". Under the GDPR, both data controllers and data processors are now subject to direct obligations in relation to personal data.

The data controller's obligation to manage its data processors is maintained but the GPDPR also introduces direct obligations on data processors.

A data processor's obligations include:

- obtaining data controller consent before sub-contracting out any data processing. The original data processor remains fully liable for data protection failures of the sub-processor (Article 26);
- maintaining a record of processing activity which (amongst other things) needs to include details of the processor and instructing controller, third country transfers and (where possible) a description of data protection security measures in place (Article 28);
- co-operating with the data protection supervisor (Article 29);
- ensuring that appropriate technical security measures are in place (Article 31); and
- notifying the data controller of any data breach (Article 30).

Article 26 also sets out the requirements of the contract between data controllers and data processors, which is much more prescriptive than those under the DPA.

Under the GDPR, data processors as well as data controllers will now be directly liable to data subjects for breaches.

Data subjects who have suffered damage as a result of a data processor's breach may now:

- complain to the supervisory authority (Article 73);
- seek compensation from the data processor (Article 77); and
- bring a court action against the data processor (Article 75).

Data processors can also be subject to fines under the GDPR (see page 33 for more information).

Scope

Definitions and Data Processors

Impact on the insurance industry

The GDPR has clarified that personal data covers circumstances where it may not be obvious to whom the data relates, such as location data or IP addresses, but it is still possible to identify an individual from that data.

ICO guidance has recently followed this approach but the clarification in the law is welcome. The insurance industry therefore needs to be aware that location data, collected in telematics boxes or wearable devices and IP addresses collected in website analytics will be caught by the GDPR.

The application of the GDPR to data processors arguably comes close to striking a much fairer balance between data controllers and data processors. It is often seen as an unfair burden on data controllers to manage their own data protection compliance obligations as well as the activities of their processors. This may well benefit insurers and brokers which as regulated entities will be, subject to a few exceptions, data controllers.

However, protracted contractual negotiations are likely as data processors will inevitably require clear contractual provisions detailing:

- the agreed relationship between the parties with respect to each aspect of the processing activity;
- the responsibilities of the data controller and data processor; and
- specific processing instructions so as to ensure their own compliance with GDPR obligations.

We anticipate that such requirements will make data processing agreements and negotiations much more complex and lengthy.

Practical steps

- Review data classifications to ensure that data which will now definitively be deemed personal data are subject to the appropriate protections.
- Ensure all data from which an individual can be identified (which will include location data and IP addresses) are covered by privacy policies and fair processing notices.
- All data processing arrangements will need to be reviewed to ensure the contracts contain:
  - all of the requirements set out in Article 26; and
  - appropriate risk allocation of liability for data breaches between data processors and data controllers.

Contract reviews should be prioritised taking into consideration volume and sensitivity of personal data that is processed.

“The application of the GDPR to data processors arguably comes close to striking a much fairer balance between data controllers and data processors. It is often seen as an unfair burden on data controllers to manage their own data protection compliance obligations as well as the activities of their processors”

Scope

Extra Territorial Effect

Current position under the DPA and ICO Guidance

The DPA has limited territorial scope. It applies to data controllers "established" in the UK. There is an accompanying limited definition of establishment. It also applies to data controllers who are processing personal data on equipment in the UK.

> "The GDPR will not only apply to data controllers established in the EU but also to those which offers goods or services to EU residents or monitor the behaviour of EU residents"

Position under the GDPR

Article 3 expands the territorial reach of European data protection legislation. The GDPR will not only apply to data controllers and data processors established in the EU but also to those which:

I. offer goods or services to EU residents (irrespective of whether a fee is charged); or

II. monitor the behaviour of EU residents as far as that behaviour occurs in the EU.

Recital 20 states that when assessing if a non-EU established business is offering goods or services to data subjects in the EU consideration needs to be given to whether the business is:

- offering services in a language or currency of a Member State;
- enabling EU residents to place orders in such other language; or
- referencing EU customers in its publications.

This may make it "apparent that the data controller envisages offering goods or services" to EU residents, and it is likely to be considered to be subject to the GDPR. Merely having a website which is accessible by EU residents is insufficient.

Monitoring the behaviour of EU residents will include tracking EU residents on the Internet in order to create profiles or to analyse or predict preferences and behaviour (if the behaviour takes place in the EU).

Businesses outside the EU caught by the GDPR will need to appoint a representative established in the EU, who shall act on behalf of the data controller or data processor and act as the point of contact for supervisory authorities.

A representative is not required if the processing is:

- occasional;
- does not include large scale processing of sensitive personal data; and
- is unlikely to result in a risk for the rights and freedoms of data subjects.

The representative may itself also be subject to enforcement action in the event of non-compliance by the data controller.

HOME

Scope

Extra Territorial Effect

Impact on the insurance industry

Given the nature of regulation of the insurance industry in the UK there is limited scope for companies established outside Europe to sell insurance to customers located in the EEA without being authorised (the exact requirements depend on the law in each Member State). It is therefore unlikely that the widening of the scope of data protection law to cover companies outside the EEA will have a significant effect on the insurance industry outside the EEA. Nevertheless, it is worth noting this extension in scope. For example, an insurance broker located in Florida marketing its services to EU citizens with holiday homes in Florida might find itself subject to the GDPR, although how easy it would be to enforce is another matter.

Practical steps

Data processing arrangements will need to be reviewed to ensure the contracts contain:

- all of the requirements set out in Article 26; and
- appropriate risk allocation of liability for data breaches between data processors and data controllers.

> “It is unlikely that the widening of the scope of data protection law to cover companies outside the EEA will have a significant effect on the insurance industry outside the EEA”

Principles and Processing

Fair Processing Information

Current position under the DPA and ICO Guidance

The DPA states that in order for the processing of personal data to be fair, the data controller must provide fair processing information which states:

- the identity of the data controller;
- the purposes of the processing; and
- any further information which is necessary to make the processing fair.

This obligation does not apply if providing the information would involve disproportionate effort or if the data are processed to meet a legal obligation of the data controller.

There are also a number of exemptions in the DPA which mean that the information does not need to be provided in specific circumstances. For example, if the provision of the information would prejudice the prevention or detection of crime.

The Directive however contained more prescriptive obligations which did not make it into the DPA including that:

- if the data are obtained directly from the data subject, the notice must state whether replies to questions are obligatory or voluntary, as well as the possible consequences of the failure to reply; and
- if the data are not obtained directly from the data subject, the notice must list the categories of data being processed.

The DPA also does not prescribe any format requirements for notices, although the ICO has provided some guidance in its Privacy Notice Code of Practice. The Code of Practice contains general principles regarding the format and drafting style of privacy notices which broadly align with the GDPR, for example stating that notices should be drafted clearly in an easy to understand manner for the intended recipient.

Position under the GDPR

The GDPR requires a significant increase in the information to be provided by data controllers to data subjects.

Article 12 states data controllers shall have transparent and easily accessible information notices; and provide information in a concise form, using clear and plain language.

The GDPR envisages that information may be provided using standardised icons. This will be subject to the future adoption of delegated acts by the European Commission.

In addition to the requirements contained in the Directive and the DPA, data controllers must also provide:

- the contact details of the data controller;
- the contact details of the Data Protection Officer (if any);
- the legal basis (as well as the purpose) of the processing, and:
  - whether the provision of personal data are required by law or for a contract, as well as whether the data subject is obliged to provide the data and the possible consequences of the failure to provide such data; or
  - if the processing is based on the controller's legitimate interests, an explanation of those interests; or
  - if the processing is based on consent, the right to withdraw consent at any time;
- the data retention period;
- a reference to the rights to erasure, to object to processing, data portability and to complain to the supervisory authority;
- information on international transfers and the safeguards applied to such transfers; and
- the existence of automated decision making (including profiling) and the envisaged consequences of such processing for the data subject.

Where the personal data are not obtained directly from the data subject, the notice should also identify the categories of personal data concerned and the source of the data.

The GDPR also sets out detailed requirements for when such information should be provided which depends on whether the data are collected from the data subject themselves or from a third party.

HOME

Principles and Processing

Fair Processing Information

Impact on the insurance industry

All privacy notices will need to be reviewed and amended in preparation for the implementation of the GDPR. Particularly challenging obligations for the insurance industry will be to specify:

- processing grounds relied upon; and
- data retention periods.

It is likely that a large degree of preparatory work will be required to establish this information before it can be translated into privacy notices.

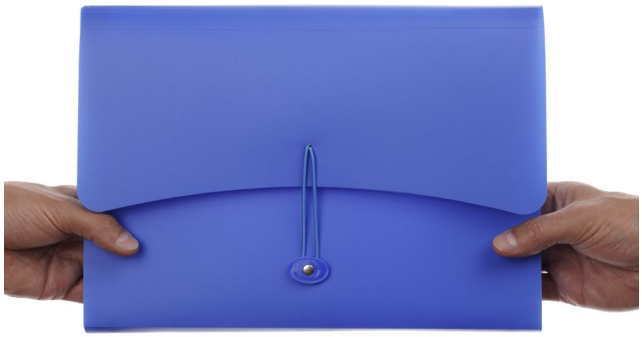
Where personal data are received from a third party the recipient will need to give consideration as to how a notice can be provided to the data subject for compliance with the GDPR, particularly where the arrangements with the third party limit the circumstances in which the data subject can be contacted directly. Contractual arrangements with such third parties may therefore need to permit the provision of an appropriate privacy notice.

Privacy notices will now need to specify the source of the information. It is not clear if the source will need to be specifically identified, or whether a generic reference to the source being, for example, "your insurance broker", will suffice – updated guidance from the ICO on drafting privacy notices for compliance with the GDPR is awaited.

For businesses in the insurance industry, it is common for the privacy notice to be provided using a layered approach with shorter privacy notices contained in application forms, policy wordings and claims forms which direct individuals to a longer form notice on the data controller's website. This approach will still be permissible under the GDPR. Alternatively, locating all of the information in one privacy notice is an approach which remains compliant with the requirements of the GDPR.

Practical steps

- Businesses should begin reviewing their privacy notices (including telephone notices) to assess what information is required by the GDPR but is not currently provided.
- Data retention periods and legal grounds for processing should be established and documented ready for inclusion in privacy notices.



> "All privacy notices will need to be reviewed and amended in preparation for the implementation of the GDPR"

Principles and Processing

Processing Conditions and Exemptions

Current position under the DPA and ICO Guidance

Principles

The DPA contains eight principles summarised as follows:

1. fair and lawful processing;
2. purpose limitation;
3. adequate, relevant and not excessive;
4. accurate and up to date;
5. not kept longer than necessary;
6. processed in line with data subject rights;
7. appropriate security;
8. restrictions on extra EEA transfers.

Processing Conditions

In order to process personal data in compliance with the DPA the relevant processing conditions must be met.

A processing condition from Schedule 2 of the DPA is always required for the processing of personal data. Where sensitive personal data are being processed, an additional processing condition is required as set out in Schedule 3 of the DPA and in a number of additional statutory instruments.

Exemptions

The DPA provides exemptions to certain obligations in specific circumstances. These exemptions broadly relate to:

- registration with the ICO; and/or
- granting access to a data subject's personal data; and/or
- obligation to process personal data fairly (i.e. to give privacy notices); and/or
- the restriction on disclosing personal data to third parties.

There are certain other specific exemptions e.g. processing in the employment context.

Position under the GDPR

Principles

The principles remain largely untouched, with the exception of the addition of a new principle of accountability (see page 25 for further details).

Principles 6 and 8 of the DPA remain in substance, but no longer in the form of a principle.

Processing Conditions

The processing conditions also remain largely untouched. However, the requirements for validly obtaining consent have been increased to place a higher burden on data controllers. Any consent relied upon to process personal data must be unambiguous.

Article 7 sets out what is meant by consent:

- data controllers must be able to demonstrate that consent was given;
- where consent is given in a written declaration which also concerns other matters (e.g. a contract) the request for consent must be clearly distinguishable, intelligible and easily accessible. If this requirement is not complied with, the consent will not be binding;
- data subjects need to be informed of their right to withdraw consent at any time and it must be as easy to withdraw consent as give it;
- when assessing if consent has been freely given "utmost" account should be taken of the fact that performance of a contract is conditional on the provision of consent to processing data that is not necessary for the performance of a contract.

Affirmative action to show consent can still be given by ticking a box or choosing appropriate technical settings. Silence and pre-ticked boxes do not constitute consent.

Where consent is relied on for the purposes of processing sensitive personal data, consent must be explicit. As the requirement for consent is now so high, the line between what constitutes consent and what constitutes explicit consent becomes ever more blurred. We await further guidance on what, if any, distinction there is.

Exemptions

The GDPR gives Member States a large amount of discretion to determine their own exemptions to the provisions of the GDPR in respect of processing data for various 'public interest' purposes such as national security.

Further legislation and guidance on this is awaited but we think it is unlikely that the exemptions set out in the DPA will be narrowed in any material way.

HOME

Principles and Processing

Processing Conditions and Exemptions

Impact on the insurance industry

Despite much lobbying by the insurance industry, the processing conditions which permit the processing of sensitive personal data were not expanded to include processing of sensitive personal data when necessary for the purposes of a contract. Whilst this was not a processing condition for sensitive personal data under the DPA, the stricter requirements on obtaining consent under the GDPR will mean consent will be very difficult to obtain for any ancillary purposes.

This means that where the insurance industry is processing health data, for example, for the purposes of underwriting health insurance, explicit consent that meets the Article 7 requirements will need to be obtained.

In particular, Article 7(4) requires data controllers to take "utmost account" of whether the performance of a contract is conditional on the provision of consent. Clearly in the case of underwriting health insurance, the performance of the insurance contract must be conditional on the data subject giving their explicit consent to the processing of sensitive personal data. However, data controllers cannot rely on that consent to process sensitive personal data for other reasons e.g. profiling.

Practical steps

- Assess all processing of personal data currently undertaken and determine whether consent is relied upon as a processing condition. Where personal data and sensitive personal data are processed on the basis of consent consider whether an alternative processing condition can be relied on. If not:
  - where personal data are processed on the basis of consent ensure the requirements for consent are complied with including by ensuring that privacy notices clearly explain why the data are needed and what it is used for;
  - where sensitive personal data that is necessary for the performance of a contract are processed on the basis of explicit consent, ensure the requirements for explicit consent are complied with including by ensuring that privacy notices clearly explain why the data are needed and what it is used for;
  - where sensitive personal data that is not necessary for the performance of a contract are processed on the basis of explicit consent (e.g. profiling), ensure that privacy notices clearly identify this processing and allows the data subject to easily refuse to provide consent. If consent is given, it should be capable of being easily withdrawn.
- Records of processing conditions relied upon must be maintained in all circumstances. In particular, where consent is relied upon records of the actual consent must be maintained.
- Records of exemptions relied upon must also be maintained in all circumstances.

> "The line between what constitutes consent and explicit consent becomes ever more blurred"

HOME

Data Subject Rights

Profiling

Current position under the DPA and ICO Guidance

The DPA does not define "profiling"; instead it refers to "automatic decision making".

A data subject is entitled to require a data controller to ensure that no decision which specifically affects him or her is made solely based on automatic means unless such decision is made in the course of entering into or performing a contract or is authorised or required by law.

Additionally, if a decision is made by automated means, a data subject is entitled to know the methodology behind such decision as part of a subject access request.

Position under the GDPR

The GDPR introduces a new definition of "profiling" (Recital 58) which is defined as "any form of automated processing of personal data evaluating personal aspects relating to a natural person, in particular to analyse or predict aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements".

Article 20 introduces a new right not to be subject to a decision based solely on profiling which produces a legal or other similarly significant effect.

The restriction does not apply if the decision is:

- necessary for a contract;
- required by law; or
- has the explicit consent of the data subject.

There is an absolute restriction on profiling using sensitive personal data unless the data subject has given explicit consent or it is necessary for reasons of substantial public interest.

In circumstances where profiling is permitted, the data controller must implement suitable measures to safeguard the data subject's rights and interests. Additionally, a data controller who uses profiling techniques must implement appropriate technical and organisational measures to safeguard against inaccuracies and prevent discrimination.

The data subject should be informed in the privacy notice of the existence of profiling, the logic used and the significance and likely consequences of such profiling.

Impact on the insurance industry

This new right is significant to the insurance industry as the underwriting process involves systematic profiling of individuals. Big data projects with outputs including targeted marketing, fraud detection, favourable customer identification will all be affected.

Profiling activities for underwriting purposes are likely to remain permissible as they can be considered necessary for a contract. However, profiling for marketing purposes will always require explicit consent.

Practical steps

- Conduct an analysis of all current profiling activities and determine which will require explicit consent (those profiling activities which use sensitive personal data and those profiling activities which are not necessary for a contract or required by law).
- Update privacy notices to refer to profiling activities. These will need to be tailored to the particular profiling in order to specify any likely effect on the data subject.
- Consider the mechanisms required in order to obtain specific consent (see page 9).
- Ensure appropriate measures are in place to prevent profiling which produces inaccurate outcomes and measures which guard against discrimination.

HOME

Data Subject Rights

New Right of Data Portability

Current position under the DPA and ICO Guidance

There is no right of data portability or other equivalent right under the DPA. However, data subjects have a right to receive a copy of their personal data in response to a subject access request in an intelligible format.

Position under the GDPR

Article 18 introduces a new right for data subjects. 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 machine readable format; and
- not hinder the data subject's transmission of personal data to a new data controller.

Where technically possible, a data subject also has a right to require that their personal data is transmitted directly between data controllers.

The right of data portability only applies where:

- data is processed by automated means; and
- the data subject has provided consent to the processing; or
- the processing is necessary to fulfil a contract.

Impact on the insurance industry

This right will apply to most personal data held by the insurance industry as it will be held electronically, either because it is necessary for the purposes of a contract or on the basis of consent.

The right seeks to protect data subjects against lock-in effects, meaning customers can move around more. This may have an effect on customer retention on expiry of a policy.

The insurance industry needs to be prepared for such requests and to provide such data to other companies on request.

Problem areas for the insurance industry are likely to be how the data are accessed and combined into a structured, commonly used and machine readable format. Many insurers and intermediaries will hold personal data on different systems (e.g. separate underwriting and claims systems). Many also have legacy systems which may not be compatible with newer software. Telematics data may also be problematic, particularly given that a data standard has not yet been developed.

Practical Steps

- Review personal data on systems to establish how they can be provided to the data subject and to your competitors(!) on request.
- Delete personal data that are no longer required.
- Establish policies and procedures for responding to requests.

HOME

Data Subject Rights

New Right of Erasure

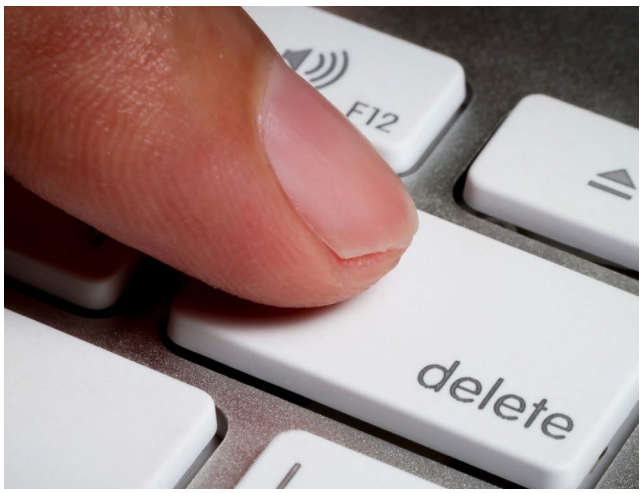
Current position under the DPA and ICO Guidance

Principle 5 of the DPA obliges data controllers to ensure that personal data is not kept longer than necessary.

Data subjects have a right to have their personal data erased:

- if the data subject can prove substantial unwarranted damage or distress; or
- by court order, when the personal data is inaccurate.

This is a high threshold and, as such, this is currently a little used right.



Impact on the insurance industry

This change is likely to have a material impact on the insurance industry which to date has sought to retain personal data for as long as possible to maximise potential use.

With the balance of power now shifted from data controller to data subject, the burden of proof is on the data controller to demonstrate the legitimate interest and/or legal and regulatory reason for data retention.

We expect data subjects will have unrealistic expectations of their rights and therefore data controllers need a clear and documented reason why they are keeping personal data.

Position under the GDPR

Article 17 provides data subjects with a new enhanced right to request their personal data. Data subjects do not need to prove substantial unwarranted damage or distress or inaccuracy.

Data controllers must delete personal data on request where specified grounds apply. Such grounds include:

- where the personal data are no longer necessary for the original purpose for which the data were collected/processed; and
- if the data subject withdraws their consent and no other legal ground for processing applies.

However, there are a number of grounds on which data controllers can rely to keep personal data. These include:

- compelling legitimate grounds;
- compliance with a legal obligation; or
- establishment, exercise or defence of legal claims.

Where a request for erasure has been received in respect of personal data which has been disclosed by the data controller to a third party, the data controller must take all reasonable steps to inform any onward data controllers of the request.

There are other provisions throughout the GDPR which require increased transparency as to how long data controllers are to keep personal data.

For example, Article 14 requires that a privacy notice contains details of the period for which the personal data will be stored. The right of subject access in Article 15 obliges a data controller to inform data subjects on request of the envisaged period for which personal data will be stored or the criteria used to determine the period. Article 28 requires data controllers to keep a record of their processing activities. This shall include information regarding the envisaged time limits for deleting different categories of data.

Practical steps

- A data retention policy should be amended to define the legal and regulatory reasons for retaining categories of personal data for specified periods of time. This policy needs to be implemented into both new and existing systems.
- Policies and procedures should be put in place documenting how erasure requests are to be handled.
- Prioritise transition of personal data from historic systems onto new systems which can be built to incorporate data retention and destruction rules.

HOME

Data Subject Rights

The Best of the Rest

Current position under the DPA and ICO Guidance

Data subjects have a right to:

- receive their personal data in response to a subject access request in an intelligible format within 40 days of request, for a fee of £10. They also have a right to certain limited information about the processing undertaken;
- rectification of their personal data if it appears to a court to be based on inaccurate data. This requires a court order to enforce;
- prevent processing of their personal data in certain defined circumstances and where they can show such processing would cause unwarranted substantial damage or distress; and
- object to direct marketing.

Position under the GDPR

Article 15 contains an enhanced right of subject access. The right is subject to fewer conditions and data subjects can request more extensive information.

The time period for dealing with subject access requests has been reduced from 40 days to 1 month and the ability to charge a fee has been removed.

Data subjects will be entitled to more extensive information about the personal data being processed about them including the legal basis of the processing, the period of data storage, information about access and other rights over the data (including the right to lodge a complaint with a supervisory authority), details of any transfers outside of the EEA and safeguards applied to such transfers, as well as contact details of the data controller's data protection officer.

The rights of rectification and restriction of processing (Articles 16 and 17a) are now much easier to enforce and do not need a court order. These rights demonstrate a seismic shift towards giving data subjects control over their own data.

Impact on the insurance industry

With access to personal data becoming easier, it is likely that there will be an increase in subject access requests. These will require additional financial and administrative resources. The increased detail regarding the processing to which a data subject is entitled will further add to this burden.

With an increased public awareness of rights data controllers may receive an increased number of requests for restrictions on processing or rectification.

Practical Steps

- Amend subject access request policies and procedures to take account of increased rights, amended timescales (including how quickly data processors should be required to pass on such requests) and removal of the ability to charge a fee.
- Develop new policies for prompt rectification of personal data and a procedure to cease processing where applicable.

HOME

Accountability

General Policies and Records

Current position under the DPA and ICO Guidance

There is no general principle of accountability under the DPA.

The ICO may request copies of appropriate data protection and information security policies when investigating complaints and may also issue sanctions to data controllers who do not have such policies in place. However, there is no specific requirement for such policies under the DPA. Sanctions are issued on the basis that appropriate technical and organisational measures were not in place in breach of principle 7 (security).

Position under the GDPR

Article 5 introduces a new principle of accountability. Data controllers are responsible for and must be able to demonstrate compliance with the principle of accountability. There are many obligations throughout the GDPR which require documentation to be kept, which will need to be produced to a supervisory authority on request.

Article 22 states that appropriate technological and organisational measures should be in place to ensure that processing is conducted in compliance with the GDPR. Data controllers should be able to demonstrate this and the measures should be reviewed and updated where necessary. The measures in place shall include the implementation of appropriate data protection policies.

Article 28 obliges both data controllers and data processors to maintain records of processing activities. Such records need to include details such as data retention periods, extra EEA transfers of personal data and the recipients of personal data. These need to be made available to a supervisory authority on request.

> “There are many obligations throughout the GDPR which require documentation to be kept, which will need to be provided to a supervisory authority on request.”

Impact on the insurance industry

While the principle of accountability is a new concept under data protection law, the insurance industry is already required to have appropriate systems and controls in plcae to manage its operational risk.

Such systems and controls should be reviewed to ensure they adequately address the principle of accountability in sufficient detail to meet the requirements under the GDPR.

Practical steps

- An audit should be undertaken of all systems processing personal data and the purposes for which the personal data are processed. Detailed records should be kept to record this activity, its outcomes and any action to be taken.
- A programme of ongoing monitoring should be established.
- All data protection policies and procedures should be reviewed in light of the new principle of accountability.

HOME

Accountability

Data protection by design and by default

Current position under the DPA and ICO Guidance

Principle 7 states that appropriate technical and organisational measures shall be taken to prevent unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The interpretation of this principle states that regard should be had for the state of technological development, the cost of implementing the measures, the nature of the data and the harm which may result.

No further details are specified in the DPA.

Position under the GDPR

Article 23 introduces the concepts of data protection by design and by default which are much more specific than the current general obligation to have appropriate security in place under the DPA.

'Data protection by design' requires data controllers to implement appropriate technical and organisational measures to protect the rights of the data subject and ensure compliance with the GDPR, having regard to the technology required to meet this obligation and the costs of implementation of the same, the nature, scope and purpose of the processing, as well as the risks posed to the data subject of the processing activities. Pseudonymisation is referred to as a good example of data protection by design (see page 31 for further detail).

'Data protection by default' means data controllers must implement appropriate technical and organisational measures to ensure that only personal data that is necessary for processing for a specific purpose is processed. To comply, data controllers should take into account:

- the amount of data collected;
- the extent of the processing;
- the period of storage; and
- the accessibility to that data.

Data controllers should ensure that, by default, personal data is not made available or accessible to an indefinite number of individuals.

Impact on the insurance industry

A culture of data protection by design and by default will need to be embedded across all business areas to ensure that data protection is considered at the very first step of any new business planning and at every stage thereafter.

The first step to encouraging such behaviour will be to ensure that staff are adequately trained in data protection compliance issues. This is likely to result in an additional cost to insurers.

Practical steps

- All new systems should be built using data protection by design and by default. In practice this will mean ensuring that there is the technical functionality to implement the requirements of the GDPR. For example, systems should be capable of searching for and extracting all personal data of a particular data subject in order to comply with the right of data portability.
- Businesses should visibly embed data protection in their culture at every level (e.g. by reference to data protection in corporate values and training of employees).

Accountability

Privacy Impact Assessments

Current position under the DPA and ICO Guidance

There is no legal requirement that data controllers carry out a privacy impact assessment (**PIA**). However, to our knowledge, the ICO is the only data protection authority in Europe who has produced guidance encouraging data controllers to conduct PIAs as a tool to demonstrate compliance with their obligations under the DPA. Guidance was issued by the ICO in 2007 and subsequently updated in 2014.

> "The mandatory requirement to carry out a PIA in certain circumstances will add an extra compliance step in the process of rolling out new data projects."

Impact on the insurance industry

Many of our clients have already started to carry out PIAs. However, the mandatory requirement to carry out a PIA in certain circumstances will add an extra compliance step in the process of rolling out new data projects. This will need to be budgeted for both in terms of time and costs. There is a chance that increased communication with the ICO in respect of "high risk" projects could, in turn, bring the ICO's focus specifically to an organisation's general data protection compliance.

Position under the GDPR

Article 33 introduces a requirement that PIAs are performed where processing activities present a "high risk" to the rights and freedoms of individuals.

The GDPR sets out a particular list of activities which will trigger the need to carry out a PIA prior to the processing of that personal data. The list is non-exhaustive and includes:

- activities which are systematic and extensive and which use automated processing of personal data in order to evaluate, analyse or predict behaviour;
- the large scale processing of sensitive personal data; and
- the systematic monitoring of publically accessible information on a large scale.

In addition, each supervisory authority is required to establish and make public a list of the types of processing activities which do and do not require a PIA.

The GDPR states that the data controller should seek the advice of the data protection officer when carrying out a PIA.

The PIA should contain:

- a description of the processing, including the legitimate interest pursued by the data controller;
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the safeguards and measures to protect against those risks.

The PIA should be reviewed whenever there is a change to the risks presented by the processing operations.

If a PIA indicates that the processing would result in a high risk to a data subject, in the absence of steps taken by the data controller to mitigate the risk, prior consultation with its supervisory authority is required.

Practical steps

- Prepare a template PIA and train relevant employees in its use.
- Begin to carry out a PIA in relation to each new data processing project and ensure that outcomes and compliance steps are documented and actioned.
- Look out for ICO guidance on when a PIA will or will not be required.

HOME

Data Protection Officers

Data Protection Officers

Current position under the DPA and ICO Guidance

Neither the DPA nor any ICO guidance obliges data controllers to appoint a data protection officer. However, in reality most large organisations have at least one data protection officer or a team of data protection specialists.

Impact on the insurance industry

According to paragraph 7 of the introduction to the GDPR, the mandatory appointment of DPOs was agreed as being required only in strictly limited circumstances. However, the wording of the provisions means this is likely to be far wider reaching and could catch the majority of large organisations. It is likely to include most large insurers and brokers, especially those who are using any monitoring devices to collect personal data (e.g. smartphones, apps and wearable devices, drones) from insureds and later processing the data through data analytics.

In practice, the majority of the insurance industry has DPOs in place, however job specifications will need to be reviewed in light of those requirements specified in the GDPR.

Practical steps

- Review the current job specification of your organisation's DPO and consider whether it is appropriate in light of new requirements specified in the GDPR.
- Consider the practical issues surrounding the DPO appointment (e.g. independence, separate function to legal, separate budget, report directly to the board).
- Consider any jurisdictional issues involved with the appointment and whether multiple DPOs should be appointed to cover different jurisdictions.
- Depending on the size of your organisation, consider whether the DPO is likely to require a support team in order to carry out their role effectively and meet all the obligations of the GDPR.

Position under the GDPR

Article 35 obliges both data controllers and data processors to appoint DPOs in three situations:

- where they are a public body;
- where core activities require regular and systematic monitoring of personal data on a large scale; and
- where core activities involve large scale processing of sensitive personal data.

Group companies can appoint a single DPO, provided the DPO is easily accessible from each establishment.

DPOs must be selected on the basis of professional qualities and expert knowledge of data protection law but do not need to be legally qualified. DPOs can be either an employee or contractor.

DPOs must be informed of all data protection issues within the organisation in a proper and timely manner. DPOs must be provided with the necessary resources to carry out his/her tasks and have access to all personal data and processing operations.

The minimum duties of a DPO include:

- informing and advising the data controller or data processor and employees processing personal data of their obligations;
- monitoring compliance with the GDPR and any other relevant EU or national legislation;
- cooperating with the applicable supervisory authority and acting as the contact point for any issues that arise; and
- advising on privacy impact assessments and monitoring their impact.

The DPO shall be independent from the data controller or data processor that appoints him or her, and specifically must not be instructed on how to carry out the required tasks listed above. The DPO must report directly to the highest level of management and shall not be dismissed or penalised for performing his/her tasks. This effectively provides the DPO with a special "protected status" within an organisation, and may create challenges for employers if there is a need to take legitimate performance management or other action against a DPO in the context of the employment relationship.

DPOs can carry out other tasks alongside their data protection duties, however, the employer is required to ensure there are no conflicts of interest in the execution of such duties.

HOME

Breach Notification

Breach Notification

Current position under the DPA and ICO Guidance

With the exception of communication and internet service providers, there is no obligation to report breaches of security to the ICO or data subjects, although ICO guidance recommends that "serious" breaches are reported to both the ICO and data subjects.

The ICO considers voluntary notification to be a mitigating factor when considering the level of monetary penalty to be imposed.

Position under the GDPR

Article 31 introduces mandatory data breach reporting. Data controllers will be obliged to report security breaches to the relevant supervisory authority "without undue delay, and where feasible, not later than 72 hours" after it first becomes aware of it. If the notification is made after 72 hours, a reasoned justification for the delay must be provided.

However, it is not necessary to notify the breach where it is "unlikely to result in a risk for the rights and freedoms" of data subjects.

Article 32 provides that security breaches must also be notified to data subjects where the breach "is likely to result in a high risk" to the rights and freedoms of data subjects.

However, notification to data subjects is not required if:

- the data controller has implemented appropriate security measures that render the data unintelligible to any unauthorised person, such as encryption; or
- the data controller has taken subsequent measures to ensure the high risk to data subjects does not materialise; or
- it would involve disproportionate effort, in which case a public communication will suffice.

Impact on the insurance industry

It is vital for every organisation to have a data breach response plan in place to enable a quick reaction to identify and contain a breach and notify the ICO, ideally within the 72 hour period.

Cyber liability underwriters should consider whether mandatory reporting requirements might lead to an increase in claims being brought against companies where previously data subjects may not have been aware that a security breach had even occurred.

Practical steps

- Review policies and procedures to ensure that data breaches can be detected and managed promptly, in order to be able to comply with the new notification requirements.
- A response plan should be put in place in order to map out key roles and responsibilities, which will save time and confusion if a breach occurs.
- Underwriters should consider the increased risk of claims when underwriting and pricing policies that include cover for data breaches.
- Consider cyber insurance options.

HOME

Security

Security measures

Current position under the DPA and ICO Guidance

Principle 7 states that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The interpretation of that principle states that this should have regard to the state of technological development, the cost of implementing the measures, the nature of the data and the harm which may result. No further specifics are given.

ICO guidance has been produced over the years outlining good and bad practice. Undertakings, enforcement notices and monetary penalty notices also give good guidance as to security measures and training that the ICO expects as a minimum standard.

Position under the GDPR

Article 5 requires personal data to be processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using technical or organisational measures. It applies to both data controllers and data processors.

Article 30 provides greater detail as to what amounts to "appropriate" technical and organisational measures. The GDPR requires data controllers and data processors to balance the changing state of technology, the costs of implementation, the risks presented by the data processing and consequences of breach for data subjects, and implement a level of security appropriate to the risk, including:

- pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;
- the ability to quickly restore the availability and access to data in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of security measures.

It is also worth remembering that all security measures taken need to comply with the concept of privacy by design and by default, and should be regularly reviewed to ensure that they remain appropriate.

Impact on the insurance industry

The insurance industry will generally already have robust security measures in place. Therefore, although the GDPR provides further guidance on what these measures should look like, many insurers and brokers will find that they already meet the requirements.

Practical steps

Insurers should be carrying out a review of the security measures in place to ensure that they are appropriate to the nature of the data held, and the risk of impact on data subjects if a breach were to occur. Particular regard should be had to whether it is appropriate to pseudonymise or encrypt the data. It should also be highlighted that this should not be a one off task – the review process should be carried out regularly to ensure the security measures remain effective and appropriate in light of changing technology.

HOME

Security

Anonymous and Pseudonymous Data

Current position under the DPA and ICO Guidance

There is no definition in the DPA of anonymous or pseudonymous data.

In 2012 the ICO produced an anonymisation code of practice which defined anonymised data as:

"*Data in a form that does not identify individuals and where identification through its combination with other data is not likely to take place*".

There is no formal recognition of pseudonymous data. However it is commonly referred to as data from which the identity of an individual is removed, but it can be recovered, e.g. from a numerical identifier.

Position under the GDPR

The GDPR introduces definitions of anonymous and pseudonymous data.

Anonymous data is defined as "information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable" (Recital 23).

"Pseudonymisation" means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person (Article 4(3b)).

Despite being considered personal data (and therefore being generally subject to the GDPR's personal data requirements), the use of pseudonymisation as a data security method is supported by the GDPR because it is recognised as being able to "reduce the risks for the data subjects concerned". It is also a recognised process in implementing data protection by design.

There are benefits to companies utilising pseudonymisation:

- it is a positive factor when determining whether a future data use is "compatible" with the original use for which the data were gathered (Article 6(3a));
- in the event of a data breach affecting pseudonymised data, data subjects may not need to be informed if the "key" that would allow re-identification was not compromised.

Impact on the insurance industry

It had been hoped that there would be a relaxation of the requirements in respect of pseudonymised data (as indicated by prior GDPR drafts). This has not been realised in the compromise text.

However, many in the insurance industry already use pseudonymised data and will now be able to rely on its formal recognition as a valid security measure.

With the formal recognition of pseudonymisation as a security technique, it seems likely that the ICO could start penalising companies who suffer a data breach if the data was in fully identifiable rather than pseudonymised form.

Practical steps

- Where possible, personal data that is no longer required for provision of services or regulatory reasons should be anonymised. This will take it outside the scope of the GDPR and will allow businesses to use such data as they choose.
- Where personal data cannot be anonymised, businesses are advised to apply pseudonymisation as a security measure.

HOME

International Transfers

International Transfers

Current position under the DPA and ICO Guidance

Principle 8 states that personal data should not be transferred outside of the EEA unless there is adequate data protection.

A transfer is permitted under the DPA if:

- the jurisdiction has been deemed adequate by the European Commission;
- an approved mechanism is used (e.g. model clauses); or
- a derogation applies (e.g. consent of the data subject).

In addition, a number of jurisdictions go further and also require notification or approval of the transfer by the local data protection authority.

Position under the GDPR

Articles 40 – 45 leave the current position largely unchanged.

The following additions should be noted:

- the European Commission can deem a particular sector (e.g. financial services) in a particular jurisdiction as adequate;
- binding corporate rules are specifically acknowledged;
- there are two new approved mechanisms of transfer – reliance on an approved code of conduct or an approved privacy seal;
- a new derogation has been inserted which permits a transfer when in the legitimate interests of the data controller and where:
  - the transfer is not repetitive and only concerns a limited number of data subjects; and
  - the controller has assessed the transfer, adduced safeguards and has a "compelling" legitimate interest that is not outweighed by the interests or rights and freedoms of the data subject.

Importantly, local data protection authorities are prohibited from requiring additional notification or approval of a transfer if the transfer is made under a European Commission decision of adequacy or appropriate safeguards specified in the GDPR are met.

Impact on the insurance industry

The changes are positive for the insurance industry. Insurers with a number of European establishments often have to undertake complex projects to notify or seek approval from multiple local data protection authorities in order to send data to group companies or service providers located outside of the EEA. This is the case even when the transfers are made on the basis of the model clauses. This process will no longer be required which will reduce both costs and timeframes involved in large data transfer projects.

The GDPR also offers a simpler administrative pathway under the "lead authority" structure, which could see binding corporate rule approval times shortened.

Practical steps

- Review data flows to ensure that appropriate transfer mechanisms are in place.
- If data transfer projects which currently require notification to or approval of a local data protection authority are scheduled, consider whether it is appropriate to delay roll out until the GDPR is implemented.
- Consider whether your organisation could benefit from binding corporate rules.

HOME

Enforcement

Current position under the DPA and ICO Guidance

The DPA empowers the ICO to issue enforcement notices, assessment notices, information notices and determinations. Compulsory audits can only be performed on NHS and other government bodies. The power to issue monetary penalties of up to £500,000 for serious breaches was given in April 2010.

The highest fine to date has been £325,000. The majority of fines in the UK have been for breach of principle 7 (security) but there has been one fine for breach of principle 4 (accuracy) and one for principle 1 (fairness).

Fines can only be imposed against data controllers and not data processors.

There are a limited number of criminal offences under the DPA which can be prosecuted by the ICO through the courts.

An organisation which has an "establishment" in a Member State deals with the supervisory authority of that Member State. Group structures with establishments across Europe therefore have to deal with multiple regulators.

Position under the GDPR

Powers

Article 53 significantly increases the level of fine which can be issued, widens the circumstances in which a fine should be issued and provides supervisory bodies with additional investigative and corrective powers. Fines can be issued against both data controllers and data processors.

Additional powers granted to the ICO will include the ability to:

- carry out audits; and
- issue orders to cease operations, notify data subjects of a breach, rectify, restrict or erase data, suspend or prohibit processing or order suspension of data flows to third countries.

Criminal sanctions

Member States can put in place criminal sanctions for infringements of the GDPR.

Circumstances for a monetary penalty

Fines can be imposed for "any infringement" of the GDPR.

A warning should only replace a fine in the case of a minor infringement or where a fine would be deemed a "disproportionate burden to a natural person".

The GDPR provides a list of the considerations a supervisory authority shall take into account when assessing the level of fine to be imposed. These include:

- nature, seriousness and length of the infringement;
- nature of the processing and categories of data involved;
- number of data subjects affected and level of damage suffered;
- evidence of intention / negligence;
- mitigation;
- technical and organisation measures implemented by data controller or data processor;
- relevance of previous infringements;
- manner in which the supervisory authority became aware of the infringement(s);
- adherence to approved codes of conduct; and
- other relevant aggravating or mitigating factors.

Level of monetary penalties

When imposing fines supervisory authorities must ensure they are "effective, proportionate and dissuasive".

HOME

Enforcement

The level of fine applicable depends on the Article of the GDPR that has been breached. The fine may be levied by reference to the turnover of an "undertaking". **Full details are set out on page 35.**

The GDPR introduces some uncertainty by its use of the word "undertaking". It is an open-ended concept, which encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed (European Court of Justice Case C-41/90). If there is a breach of competition law, fines levied on an undertaking are based on its turnover in the relevant market affected by the conduct. If the relevant market is worldwide the fine is based on the worldwide turnover of the undertaking. If the relevant market is smaller (e.g. one country) the fine will be levied by reference to the turnover in that smaller market.

One stop shop and responsibility for enforcement

The much publicised "one-stop shop" has survived in a watered-down form in Article 51a. For organisations with entities in more than one Member State, the supervisory authority in the Member State of the organisation's main establishment is deemed competent to take the lead in dealing with any enforcement issues.

The lead supervisory authority will be required to consult with other supervisory authorities whose nationals are affected.

The GDPR also creates a super regulator in the form of the European Data Protection Board (**EDPB**) (formerly Working Party 29). The EDPB will include the head of each national supervisory authority and the European Data Protection Supervisor. The EDPB will issue guidance, ensure consistent application of the GDPR and be empowered to resolve disputes among the national supervisory authorities.

Impact on the insurance industry

The increase in fines and the range of circumstances in which they can be imposed will mean that data protection compliance needs to regularly be on the boardroom agenda. We expect to see data protection issues being given the same scrutiny as has previously only been afforded to financial services regulation.

Although the one stop shop mechanism should have had a positive impact, the watered down version that appears in the GDPR will disappoint many multionationals in the insurance industry as it looks like supervisory authorities in all relevant Member States will still need to be consulted in the event of a data breach which affects their nationals.

For cyber laibility insurers, the potential for data processors to be the subject of fines will impact potential exposure.

Practical steps

- Start taking all the practical steps in the other sections of this guide to avoid a monetary penalty notice!
- When underwriting cyber policies, establish whether the insured is a data controller or data processor in order to understand the appropriate risks.

> "When imposing fines supervisory authorities must ensure they are "effective, proportionate and dissuasive". The level of fine applicable depends on the Article of the GDPR that has been breached"

HOME

Enforcement

Enforcement

Level	Amount	Relevant articles
1	EUR 10,000,000 or in case of an undertaking 2% total worldwide annual turnover in the preceding financial year (whichever is greater)	■ 8: Child's consent ■ 10: Processing not requiring identification ■ 23: Data protection by design and by default ■ 24: Joint controllers ■ 25: Representatives of controllers not established in EU ■ 26-28 & 30: Processing ■ 29: Co-operation with the supervisory authority ■ 31: Notification of breaches to supervisory authority ■ 32: Communication of breaches to data subjects ■ 33: Data protection impact assessment ■ 34: Prior consultation ■ 35-37: DPOs ■ 38a(4): Monitoring approved codes of conduct ■ 39 & 39a: Certification
2	EUR 20,000,000 or in case of an undertaking 4% total worldwide annual turnover in the preceding financial year (whichever is greater)	■ 5: Principles for processing personal data ■ 6: Lawfulness of processing ■ 7: Conditions for consent ■ 9: Processing special categories of personal data (i.e. sensitive personal data) ■ 12-20: Data subject rights: to information, access, rectification, erasure, restriction of processing, data portability, object, profiling ■ 40-44: Transfers to third countries ■ 53(1): Requirement to provide access to supervisory authority ■ 53(1b): Orders / limitations on processing (definite or temporary) or the suspension of data flows ■ Obligations adopted under Member State law (specific data processing situations)

HOME

Compensation

Compensation for Data Breaches

Current position under the DPA and ICO Guidance

Claims for compensation for data breaches can only be brought against data controllers.

Section 13(1) provides that individuals that suffer material damage as a result of a breach of the DPA are entitled to compensation from the data controller.

Section 13(2) provides that individuals are entitled to compensation for distress arising from breaches of the DPA if the individual also suffers damage as a result of the breach. This had previously been interpreted to mean "material damage", which meant that individuals could only seek compensation for distress arising from data breaches if they had also suffered some financial loss. In 2015, the Court of Appeal in the case of *Vidal-Hall v Google* recognised that this distinction was somewhat artificial and ruled that individuals are entitled to claim for damages for pure distress caused by breaches in the DPA.

Impact on the insurance industry

The clarification that compensation is available for both material and immaterial damage simply confirms the law as stated by the Court of Appeal in Vidal-Hall v Google, so the changes will not be a surprise to the insurance industry.

For those insurers writing cyber insurance policies, note the potential for data processors to be the subject of compensation claims, meaning the risk of covering companies who are acting as data processors, will now increase.

Position under the GDPR

Article 75 provides that data subjects have a right to a judicial remedy against data controllers and data processors.

Article 77 provides that any person who has suffered material or immaterial damage as a result of an infringement of the GDPR shall have the right to receive compensation from the data controller or data processor for the damage suffered.

Therefore, damages will be available for pure distress claims arising from breaches of the GDPR and claims can be brought both against data controllers and data processors. A data processor's liability is limited to damage caused by its processing where it has not complied with its specific obligations under the GDPR or acted contrary to the lawful instructions of the data controller.

The burden of proof is on the party that is responsible for the event which has caused the damage.

Where multiple data controllers or data processors are involved in data processing, if any one of them is responsible for any of the damage, then it will be responsible to the data subject for all of the damage. The party which compensates the data subject will have the right to claw back compensation from the other data controllers or data processors for the damage caused by their breach.

Practical steps

- Start taking all the practical steps in the other sections of this guide to avoid a compensation claim!
- When underwriting cyber policies, establish whether the insured is a data processor or controller in order to understand the appropriate risks.

HOME

Our data protection team

Rhiannon Webster

Rhiannon is the head of DAC Beachcroft's information law advisory practice and has particular expertise in advising on data protection issues in the insurance sector. She holds the ISEB qualification in data protection law.

Rhiannon advises on a full range of data protection issues and offers strategic advice on large projects such as implementing global IT platforms; data protection issues in new technologies such as cloud services, telematics, big data initiatives and the internet of things and data security breach management including representing clients in their communications with the ICO and other regulators. She has a much sought-after practical and commercial approach to providing data protection advice.

Hans Allnutt

Hans Allnutt leads DAC Beachcroft's cyber risk and breach response team. He is an expert on cyber risk, data breach incidents and insurance policies. He has advised on a wide range of breaches and cyber incidents arising out of extortion demands, acts by malicious employees, software errors and third party negligence. He advises companies from a variety of sectors including retail, financial services, tech & telecoms, charities, higher education and healthcare.

Khurram Shamsee

Khurram is head of the London employment team and a recognised expert for data privacy and human rights issues arising in the employment context. His experience includes advising a major insurer on the data privacy implications of implementing new monitoring software impacting employees across 20 jurisdictions, and devising a unique protocol for a major retail bank to streamline their compliance with subject access requests received from both customers and employees. He has also been involved in the successful defence of civil claims pursued in connection with alleged breaches of the Data Protection Act.

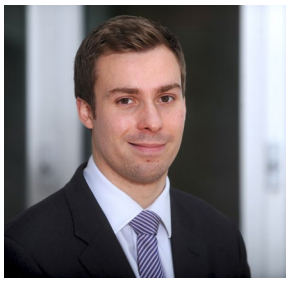
Emma Bate

Emma is a partner in our insurance advisory team and advises the insurance sector on data protection compliance. Emma's recent experience includes advising a global insurer on its involvement in a fraud initiative, involving the sharing of sensitive personal data, advising a global health insurer on the fair processing and consent notices on a European launch. Emma also advised on data protection law in a Court of Appeal case for Equifax, a credit reference agency. DAC Beachcroft successfully defended Equifax from a claim that it had failed to use reasonable steps to keep its records up to date.

Geetu Bhan

Geetu is an expert in data protection and holds the BCS (formerly ISEB) qualification in data protection. She regularly advises clients within the insurance industry on data protection issues primarily in the insurance distribution context. Geetu also assisted an insurer client with a remediation project following a significant data loss and subsequent fine. The project involved negotiating appropriate data protection provisions in over 100 procurement contracts.

HOME



Matthew Wixon

Matthew is a senior solicitor in our insurance advisory team and has spent a total of 21 months seconded to our insurance sector clients. He advises on the full range of commercial contract arrangements for insurers and insurance brokers and has worked on many data protection compliance projects for our insurance sector clients, including global data privacy remediation projects, the implementation of global HR IT systems and advising on the data protection compliance steps required in key territories to implement an insurance sale and administration tool.

Nicky Geary

Nicky is an employment solicitor in the London team who advises on a spectrum of employment matters, including data protection issues in the workplace. She has enjoyed two secondments to the insurance industry during her career.

Jade Kowalski

Jade is a senior solicitor in our insurance advisory team and an expert in data protection. Jade regularly advises clients in the insurance sector on a range of data protection issues including drafting privacy policies and complex data sharing arrangements. She has notable experience in undertaking privacy impact assessments in advance of the roll out of new technologies and managing data transfer projects across multiple jurisdictions. Jade holds the BCS Professional Qualification in Data Protection (formerly ISEB) Since qualification she has spent time on secondment with both Genworth and QBE.

Charlotte Halford

Charlotte has spent time on secondment with a variety of global insurers. Charlotte has advised and assisted on a range of data protection matters including providing strategic guidance on compliance with UK data protection law, drafting and advising on privacy and cookies policies, dealing with subject access requests, advising on the data protection elements of various commercial contracts and managing international data protection projects. Charlotte is also international editor of DAC Beachcroft's monthly client Information Security and Data Security Newsletter.

Helen Nuttall

Helen is an assistant in DAC Beachcroft's cyber risk and breach response team. She has experience in advising insurers on coverage in respect of breaches of data protection and privacy law, well as coordinating the response to a number of data breaches involving telecommunication providers, retailers and educational institutions. She regularly provides training on data protection and privacy law, cyber insurance and data breach response.

HOME