

# General Data Protection Regulation

25 January 2018

**Branko Bjelobaba FCII**  
Regulation & Compliance Consultant



## Branko Ltd

### FCA compliance consultants

- \* Compliance Manuals
- \* Engaging Events
- \* Tailored Solutions



## Today/Learning outcomes...

By the end of this briefing you will have gained an insight into:-

1. What the ICO does;
2. An overview of the GDPR;
3. What changes you may need to make.



## Will it be a bind?

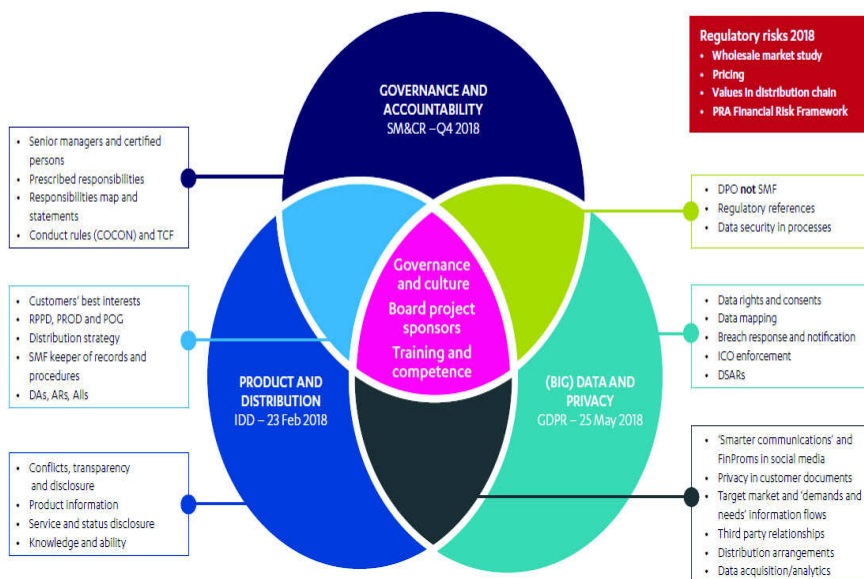
- It benefits us all, because we all own personal data. This means you have a responsibility and opportunity to show customers that you treat their information with the utmost care.
- The GDPR will force you to gain consent ethically, tighten up your security measures against cybercrime and enable you to build a new layer of trust and loyalty with customers.



# 1. Introduction



## Regulatory change 2018 – general insurance



**BBC** Sign in News Sport Weather iPlayer TV Radio More Search

# NEWS


Home UK World Business Politics Tech Science Health Family & Education Entertainment & Arts Stories More

**Business** Your Money Market Data Markets Companies Economy

## Carphone Warehouse fined £400,000 over data breach

10 January 2018

Facebook Twitter LinkedIn Email Share



### Top Stories

**Extra £44m for Calais border security**  
The UK government money will be spent on fencing, CCTV and infrared detection technology.  
1 hour ago

**Emily Maitlis fears stalker won't stop**  
2 hours ago

**PFI deals 'costing taxpayers billions'**  
16 minutes ago

**ico.**  
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home For the public For organisations Report a concern Action we've taken **About the ICO**

About the ICO / News and events / News and blogs /

## TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack

Share

Date 05 October 2016  
Type News

Telecoms company TalkTalk has been [issued with a record £400,000 fine](#) by the ICO for security failings that allowed a cyber attacker to access customer data "with ease".

The [ICO's in-depth investigation](#) found that an attack on the company last October could have been prevented if TalkTalk had taken basic steps to protect customers' information.

ICO investigators found that the cyber attack between 15 and 31 October 2015

[Subscribe](#) | [Email Newsletters](#) | [About Us](#)

[Follow @InsuranceTimes](#)


# Insurance Times

Branko Bjelobaba [Sign Out](#) [My Account](#)

September 2017 issue  
[Back issues »](#)  
[Subscribe »](#)

[»](#)

[Home](#) | [News](#) | [Analysis](#) | [Events](#) | [Top 50](#) | [Innovation](#) | [People](#) | [Research](#) | [Corporate Insight](#) | [Jobs](#) | [BSS 2017](#)

## Five sentenced for leaking Allianz UK customer data to CMCs

25 August 2017 | By Ben Dyson

[Print](#) | [Email](#) | [Share](#)

Stay informed. The latest news direct to your inbox.

[SIGN UP HERE](#)



### RELATED ARTICLES

[RSA claims specialist faces jail for defrauding his company](#)  
11 September 2017


[Man jailed for trying to defraud Hastings after CMC call](#)  
29 August 2017

[Employee data theft is the real cyber threat: Analysis](#)  
15 August 2017

### Insurance Times Jobs

- MW Appointments: Financial Lines Account Manager / Executive
- MW Appointments: Insurance Trainee
- I dex Consulting Ltd: New Business Development Executive
- I dex Consulting Ltd: Development Director
- I dex Consulting Ltd: Personal Injury Claims Handler

# So, FCA or ICO?!



BBC Sign in News Sport Weather iPlayer TV Radio More Search

**NEWS** Find local news

Home UK World Business Politics Tech Science Health Family & Education Entertainment & Arts Video & Audio More

Technology

## Equifax to be investigated by FCA over data breach

24 October 2017 Technology [f](#) [t](#) [b](#) [m](#) [Share](#)



**Top Stories**

**No heir apparent as Xi cements his power**  
Xi Jinping promotes supporters at a party congress, indicating he could rule China for a long time.  
55 minutes ago

**'Half of women' sexually harassed at work**  
8 hours ago

**All UK schools 'should have sprinklers'**  
5 hours ago

**FCA** FINANCIAL CONDUCT AUTHORITY Search

About us Firms Markets Consumers **News** Publications

Home / News / FSA fines Zurich Insurance £2,275,000 following the loss of 46,000 policy holders' personal details


## FSA fines Zurich Insurance £2,275,000 following the loss of 46,000 policy holders' personal details

Press Releases | Published: 24/08/2010 | Last updated: 29/11/2016 [Print page](#) [Share page](#)

The Financial Services Authority (FSA) has fined the UK branch of Zurich Insurance Plc (Zurich UK) £2,275,000 for failing to have adequate systems and controls in place to prevent the loss of customers' confidential information. The fine is the highest levied to date on a single firm for data security failings.

The failings came to light following the loss of 46,000 customers' personal details, including identity details, and in some cases bank account and credit card information, details about insured assets and security arrangements. The loss could have led to serious financial detriment for customers and even exposed them to the risk of burglary.

**BBC** Sign in News Sport Weather iPlayer TV Radio More... Search BBC News Q

**NEWS** 

Page last updated at 10:39 GMT, Wednesday, 22 July 2009 11:39 UK

**News Front Page**  
 World  
 UK  
 England  
 Northern Ireland  
 Scotland  
 Wales  
**Business**  
 Market Data  
 Your Money  
 Economy  
 Companies  
 Politics  
 Health  
 Education  
 Science & Environment  
 Technology  
 Entertainment  
 Also in the news  
 Video and Audio  
 Have Your Say  
 Magazine

 E-mail this to a friend  Printable version

## HSBC fined for personal data loss

**Three HSBC firms have been fined more than £3m for failing to adequately protect customers' confidential details from being lost or stolen.**



The Financial Services Authority (FSA) said customer data had been lost in the post on two occasions.

The firms concerned are HSBC Life UK, HSBC Actuaries and Consultants, and HSBC Insurance Brokers.

HSBC said it regretted the breaches, adding that no customer had reported any loss from these failures.

**Lack of training**

The FSA said that all three firms had taken action to address the concerns raised.

The FSA said HSBC Life had lost a CD containing 180,000 customers' details

**SEE ALSO**

- Personal data exposed on website  
19 Jun 09 | Business
- Pension details of 109,000 stolen  
28 May 09 | Business
- When financial data goes missing  
26 Aug 08 | Business
- HSBC loses customers' data disc  
07 Apr 08 | Business

**RELATED INTERNET LINKS**

- HSBC
- FSA

The BBC is not responsible for the content of external internet sites

**TOP BUSINESS STORIES**

- Unemployment dips to 2.47 million
- Credit Suisse offices are raided

## Fines – our sector

- FSA/FCA - £7.8m
- ICO £5.5m (max £500,000)

**ico.**  
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home For the public For organisations Report a concern Action we've taken About the ICO

**Nuisance calls and messages**  
Read about nuisance marketing trends and action we took in December.

**Company which made 75 million nuisance calls is fined**  
17 January 2018

**Statement on Just Eat incident**  
16 January 2018

**Four nuisance marketing companies fined by the ICO**  
11 January 2018  
[More news and blogs](#)

**Take action**

[Register or renew](#)

[Report a concern](#)

[Search the register](#)

[Meet the Commissioner](#)

[For the public](#)

[For organisations](#)

**ico.**  
Information Commissioner's Office

## Data Protection Register - Entry Details

**Registration Number:** Z5480933

**Date Registered:** 18 July 2001   **Registration Expires:** 17 July 2018

**Data Controller:** THE CHARTERED INSURANCE INSTITUTE

**Address:**

20 ALDERMANBURY  
LONDON  
EC2V 7HY

**This register entry describes, in very general terms, the personal data being processed by:**

THE CHARTERED INSURANCE INSTITUTE

**Nature of work - General business**

**Description of processing**

The following is a broad description of the way this organisation/data controller processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have received, check any privacy notices the organisation has provided or contact the organisation to ask about your personal circumstances.



#### Reasons/purposes for processing information

We process personal information to enable us to promote our goods and services, to maintain our accounts and records and to support and manage our staff.

#### Types/classes of information processed

We process information relevant to the above reasons/purposes. This may include:

- personal details
- family, lifestyle and social circumstances
- financial details
- employment and education details
- goods or services provided

We also process sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs of a similar nature
- trade union membership

#### Who the information is processed about

We process personal information about our:

- employees
- customers and clients
- suppliers and services providers
- advisers, consultants and other professional experts
- competitors and enquirers

The screenshot shows the Chartered Insurance Institute website. At the top, there is a navigation bar with the logo on the left and the text "Chartered Insurance Institute" in the center. To the right of the logo, there is a search bar with the text "Welcome Mr Branko Bjelobaba | My CII | Log out" and a search icon. Below the search bar, there is a link for "Advanced search". The navigation bar also contains several menu items: "Chartered", "Membership", "Qualifications", "Training", "Corporate", "Knowledge", "Consumer", "Network & Events", and "Careers".

## Communication Preferences

Tell us exactly what you would like to receive information on and how we should communicate with you by updating your preferences below. Once you have made your changes, click Save and your updates will be effective within one business day.

### My Membership

Receive all communication	Select none
Member updates/news	<input type="checkbox"/>
CPD updates	<input type="checkbox"/>
Faculty newsletter	<input type="checkbox"/>
Journal Xpress	<input type="checkbox"/>
My SMP	<input type="checkbox"/>
Parke affinity benefits	<input type="checkbox"/>

### Research and Thought Leadership

Research and reports	<input type="checkbox"/> Email <input type="checkbox"/> None
Policy updates	<input type="checkbox"/> Email <input type="checkbox"/> None
Government and regulator engagement	<input type="checkbox"/> Email <input type="checkbox"/> None
Surveys	<input type="checkbox"/> Email <input type="checkbox"/> None <input type="checkbox"/> Paper

### Local Institutes

## ICO - Goals

1. All organisations which collect and use personal information do so **responsibly, securely and fairly**.
2. All public authorities are open and transparent, providing people with access to official information as a matter of course.
3. People are aware of **their information rights** and are confident in using them.
4. People understand how their personal information is **used** and are able to take steps to protect themselves from its **misuse**.



## ICO – numbers 2015/16

- 400,000 data controllers registered
- **161,190 concerns reported**
- 17,300 cases investigated
- 16 fines totalling £2m
- 204,700 calls to helpline
- Annual fee £35 OR £500 if large (will change from 1 April 2018)
- Fee income £18.3m + £3.7m grant in aid
- Expenditure £23m



# ICO – work with firms

- 35 audits providing advice and recommendations
- 17 information risk reviews
- 36 follow-up audits
- 77 advisory visits to SMEs



March 23, 2017

## ICO to take on 200 staff as it help UK businesses to GDPR compliance



*The ICO is set to grow by 40 percent over the next two years to help with the mammoth task of making UK businesses compliant with GDPR before its comes into effect next year.*

The Information Commissioner's Office (ICO) is expected to grow its staff by 40 percent in the next few years to bear the weight of incoming European regulation.

The ICO, which governs data protection in the UK, will add 200 people to its staff of 500 who are already said to be buckling under the pressure. The office may battle with skill shortages for as long as two years as it attempts to hire all the lawyers, investigators and specialists it requires.



Information commissioner Elizabeth Denham: needs to hire 200 more staff

Elizabeth Denham, the information commissioner, appeared before the House of Lords on 8 March to discuss the implication of the EU's General Data Protection Regulation (GDPR) and the added resources her office would require.

Helping UK firms comply with the GDPR: money to be at the heart of this new employment drive

### MOST READ ON SC

1. Bring technologists quickly into leadership positions says ex GCHQ head
2. Bug in anti-malware defenses mistakenly blocks users' Google Docs files
3. £214 million in Ethereum crypto-currency virtually gone after code deletion
4. Pirates of the Caribbean: 66 years of secrets dug up in Paradise Papers

## ICO – by sector

- 46% Local Government
- 18% Central Government
- 11% Police & Criminal Justice
- 9% Health
- 7% Education
- **0.5% Private Companies (806/82)**



## ICO – reason to complain

- 18% - loss/theft of paperwork
- 17% - posted to wrong person
- 12% - emailed to wrong person
- 8% - insecure webpages
- 6% - others



## 2. GDPR



### Overview

- GDPR will apply in UK from 25 May 2018
- Replaces DPA 1998 (new UK law)
- Brexit will have no affect
- Will ensure international consistency around DP laws
- Much of DPA remains, some new and enhanced requirements



## Getting ready for the GDPR

### Step 1: Accountability and governance

#### 1.1: Awareness

Decision makers and key people in your business are aware that the law is changing to the GDPR and appreciate the impact this is likely to have. Your business has identified areas that could cause compliance problems under the GDPR and has recorded these on the organisation's risk register. Your business is raising awareness, across the organisation of the changes that are coming.

## Main areas

1. Data controllers' and processors' responsibilities
2. Data protection principles condensed
3. New rights of individuals
4. Accountability and governance requirements
5. Security breach reporting and timescales
6. Higher fines

## What data?

- GDPR applies to 'personal data' meaning any information relating to an identifiable person
- Incl name, identification number, location data or online identifier
- GDPR applies to both automated personal data and to manual filing systems



## Your website

- If your website collects personal data such as an email address, or even a cookie, which you in turn store somewhere in a database (for example, a newsletter or marketing list), you are a Data Controller
- Therefore, the way you gain consent to collect and store said data and the security built into your website will all come under scrutiny



The screenshot shows the homepage of the Information Commissioner's Office (ICO). The header features the ICO logo and the text: "The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals." Below the header is a navigation menu with links: Home, For the public, For organisations, Report a concern, Action we've taken, and About the ICO. The main content area includes a "Cookie control" notification, a "Take action" sidebar with buttons for "Register or renew", "Report a concern", and "Search the register", and a central news section with articles such as "Action taken after sensitive data leak on Twitter", "Company which made 75 million nuisance calls is fined", and "Statement on Just Eat incident".

## Principles

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.
4. Accurate and, where necessary, kept up to date.



## Principles

5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
6. 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 appropriate technical or organisational measures.



## Lawful processing?

You must identify a lawful basis before you can process personal data:-

1. Consent (enables you to cross-sell)
2. Legitimate interests (renewal?)
3. Necessity for the performance of a contract
4. If the processing is necessary for an “insurance purpose” – advising, arranging, underwriting, administering, administering a claim under, exercising a right or complying with an obligation under, an insurance contract (thus overarching substantial public interest to process Special Category Personal Data)



# Consent

- 'Consent' in this context simply refers to the way in which you ask people to hand you their personal data and you tell them what you will do with it.
- The days of pre-filled agreement checkboxes are long gone (are they?), but come May 2018, even closer scrutiny will be placed on the way you ask for someone's details.
- The consent you request must be affirmative, verifiable and abundantly clear, and the person filling out the form will have to proactively do something to provide you with theirs.
- Start looking at your sign-up forms today. Small tweaks may be all you need to undertake in this area.



A screenshot of the DMA (Data Marketing Association) website. The page features a navigation bar with icons for Curate, My Clips, Contribute, Connect, and Search. A central article titled "GDPR Consent or legitimate interest? Email marketers need both" is highlighted with a pink background. The article includes a sub-headline "How GDPR and PECR (ePrivacy) work together in email marketing" and three callout boxes: "Non-personalised dynamic email", "Personalised dynamic email", and "If all you need for your email marketing is the email address, you need marketing consent (or a customer relationship) in line with PECR (ePrivacy)". A "Related Articles" section on the right lists "GDPR: forget compliance we want success!". The footer contains "Terms and Conditions", "Privacy Policy", "Contact", and "Copyright DMA 2014 © All Rights Reserved".

# Direct marketing checklist

---

## Obtaining consent for marketing

- We use opt-in boxes
- We specify methods of communication (eg by email, text, phone, recorded call, post)
- We ask for consent to pass details to third parties for marketing and name, or clearly describe those third parties
- We record when and how we got consent, and exactly what it covers

## Marketing by email or text

- We only text or email with opt-in consent (unless contacting previous customers about our own similar products, and we offered them an opt-out when they gave their details)
- We offer an opt-out (by reply or unsubscribe link)
- We keep a list of anyone who opts out
- We screen against our opt-out list

# Consent

Must be:-

- Specific & Informed
- Clear & plain language
- Unbundled (separate from T&Cs)
- Active opt-in ONLY (not pre-ticked opt in)
- Named – your firm and any other (concerns)
- Documented
- Easily withdrawn – simple and effective



**•The individual MUST be able to understand what personal data of theirs you process. They need to know why you process it and what your legal basis for doing so is. If that legal basis is “legitimate interest”, explain what that “legitimate interest” is**

**•This will be contained in your privacy notices (or privacy policy), which should be clear and concise. The ICO produces guidance on privacy notices**



**Thank you for choosing to register with us. The Royal Opera House will process your data in accordance with the Data Protection Act 1998, and, from 18 May 2018, the General Data Protection Regulation (GDPR). The Royal Opera House will use your information for administration, marketing and charitable purposes, and will not share your personal details with third parties without your consent. If you have any comments or concerns regarding the use of your data, please contact the Data Protection Manager, Royal Opera House, Covent Garden, London WC2E 9DD.**



#### **Can we carry on using existing DPA consents?**

You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But it's important to check your processes and records in detail to be sure existing consents meet the GDPR standard.

Recital 171 of the GDPR makes clear you can continue to rely on any existing consent that was given in line with the GDPR requirements, and there's no need to seek fresh consent. However, you will need to be confident that your consent requests already met the GDPR standard and that consents are properly documented. You will also need to put in place compliant mechanisms for individuals to withdraw their consent easily.

On the other hand, if existing DPA consents don't meet the GDPR's high standards or are poorly documented, you will need to seek fresh GDPR-compliant consent, identify a different lawful basis for your processing (and ensure continued processing is fair), or stop the processing.

Our [consent checklist](#) sets out the steps you should take to seek valid consent under the GDPR. This checklist can also help you review existing consents and decide whether they meet the GDPR standard, and to seek fresh consent if necessary.

**Key GDPR provisions**  
[See Recital 171](#) (external link)

## Checklist

### Asking for consent

- We have checked that consent is the most appropriate lawful basis for processing.
- We have made the request for consent prominent and separate from our terms and conditions.
- We ask people to positively opt in.
- We don't use pre-ticked boxes, or any other type of consent by default.
- We use clear, plain language that is easy to understand.
- We specify why we want the data and what we're going to do with it.
- We give granular options to consent to independent processing operations.
- We have named our organisation and any third parties.
- We tell individuals they can withdraw their consent.
- We ensure that the individual can refuse to consent without detriment.
- We don't make consent a precondition of a service.
- If we offer online services directly to children, we only seek consent if we have age-verification and parental-consent measures in place.




### Recording consent

- We keep a record of when and how we got consent from the individual.
- We keep a record of exactly what they were told at the time.

### Managing consent

- We regularly review consents to check that the relationship, the processing and the purposes have not changed.
- We have processes in place to refresh consent at appropriate intervals, including any parental consents.

Home News Analysis Events Top 50 Innovation People Research Corporate Insight MGA17 Latest Jobs





### Insurance sector must "make friends with consent and each other" in the run up to GDPR and UK Data Protection Bill changes, says ICO's Emma Bate at the ABI's 2017 Data Conference

The insurance industry should not expect special treatment when it comes to the implementation of the EU's General Data Protection Regulation (GDPR) next year, an Information Commissioner's Office (ICO) official has warned.

Speaking at the ABI's 2017 Data Conference last week, ICO general legal counsel Emma Bate, formerly a partner at DAC Beachcroft, also urged the industry to "make friends with consent and each other".

The view from the regulator is that "you are not special," warned Bate. "We [the industry] have used and abused consent in this country for some time," she continued. "Now is the time to press the reset button."

Most popular Most commented

-  Towergate Underwriting hires big-hitter to head Europe expansion
-  Insurers welcome call to delay Insurance Distribution Directive
-  Zurich exploring sale of Endsleigh - report
-  Marsh targets UK mid market firms with new product

# Data Breaches

- Compulsory notification to ICO **within 72 hours where breach is likely to result in a risk to the rights and freedoms of individuals** (discrimination, damage to reputation, financial loss or other significant economic or social disadvantage)
- Notification to individual where high risk to their rights and freedoms
- Maximum fine - up to €20m or 4% of your global group turnover



The screenshot shows the top of the ICO website. The header includes the ICO logo, the text 'The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.', and a search bar. A navigation menu below the header has links for 'Home', 'For the public', 'For organisations' (which is highlighted), 'Report a concern', 'Action we've taken', and 'About the ICO'. The main content area is titled 'Report a breach' and includes a 'Share' button. Below the title, it states: 'Use this page to report one of the following types of breach to the ICO:'. A list of three breach types follows: 'a breach of the Data Protection Act (DPA);', 'a Privacy and Electronic Communications Regulations (PECR) security breach by a telecoms or internet service provider; or', and 'the unlawful obtaining of personal data (known as a section 55 DPA breach)'. To the right, there is a 'Further reading' section with a link to 'Data security incident trends' under the heading 'Action we've taken'. At the bottom left, there is a link for 'DPA security breach'.



Association of British Insurers

1

31 March 2017

## ABI response to ICO consultation on GDPR consent guidance

### About the ABI:

The Association of British Insurers (ABI) is the leading trade association for insurers and providers of long-term savings. Our 250 members include most household names and specialist providers who contribute £12bn in taxes and manage investments of £1.6 trillion.

### Response:

We believe that the ICO guidance is helpful and broadly appropriate. However, we are concerned that there are some insurance products and service offerings that will have no legal basis for processing special categories of personal data, particularly given the interpretation of consent. This may potentially leave people without insurance cover. It will also add excessive costs, or administrative burden, or contribute to an overly long customer journey. This response highlights our key concerns.

➤ [Explicit consent/Processing special categories of data](#)

## Industry concerns

1. Explicit consent to process special categories of data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life/orientation and conviction data) – broad general exemption for insurance business (substantial public interest) has now been included in the Bill
2. How can all third parties be named?
3. Can an individual provide consent on behalf of others – motor, health, etc?





# Industry concerns

4. Grandfathering of previous consents?
5. Direct marketing – what constitutes this and is it legitimate to undertake without any additional/specific consent as in the case of a renewal?
6. When should consents be refreshed?



The screenshot shows the official website for the Data Protection Bill [HL] 2017-19. The page includes a navigation menu with links to 'Parliamentary business', 'MPs, Lords & offices', 'About Parliament', 'Get involved', 'Visit', and 'Education'. Below this, there are links for 'House of Commons', 'House of Lords', 'What's on', 'Bills & legislation', 'Committees', 'Publications & records', 'Parliament TV', 'News', and 'Topics'. The main content area displays the title 'Data Protection Bill [HL] 2017-19' and identifies it as a 'Government Bill' sponsored by 'Lord Ashton of Hyde' from the 'Department for Digital, Culture, Media and Sport'. A 'Progress of the Bill' diagram shows the bill's journey through the House of Lords and House of Commons, with stages including First, Second, and Third readings, Committee stages, and Report stages. The House of Lords stage is highlighted in red, and the House of Commons stage is highlighted in green. The final stage is 'Royal Assent'. A 'Last event' section at the bottom indicates the '3rd reading: House of Lords | 17.01.2018'.

## ICO – 9 steps

1. Awareness
2. What information do you hold, where does it come from and with whom do you share it
3. Review (and amend) your privacy notices
4. Check your procedures to ensure they cover all individuals rights including how to delete or transfer data electronically
5. Update your subject access request procedures
6. Identify and document the lawful basis for your processing activity



## ICO – 9 steps

6. Review how you seek, record and manage consent
7. Ensure you have the right procedures to detect, report and investigate breaches
8. Research DP by design and default impact assessments and work out how and when to implement them
9. Consider whether you need to appoint a DP officer and where this role will sit within your organisation



## Today/Learning outcomes...

By the end of this briefing you will have gained an insight into:-

1. What the ICO does;
2. An overview of the GDPR;
3. What changes you may wish to make.



## Thank you for your attention

0800 619 6619

[www.branko.org.uk](http://www.branko.org.uk)

**Next events:**

**20 Feb on GDPR and SMCR**



# Preparing for the General Data Protection Regulation (GDPR)

12 steps to take now

# Preparing for the General Data Protection

## Regulation (GDPR) 12 steps to take now



**1 Awareness**  
You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

**2 Information you hold**  
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

**3 Communicating privacy information**  
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

**4 Individuals' rights**  
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

**5 Subject access requests**  
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

**6 Lawful basis for processing personal data**  
You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

**7 Consent**  
You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

**8 Children**  
You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

**9 Data breaches**  
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

**10 Data Protection by Design and Data Protection Impact Assessments**  
You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

**11 Data Protection Officers**  
You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

**12 International**  
If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

## Introduction

This checklist highlights 12 steps you can take now to prepare for the General Data Protection Regulation (GDPR) which will apply from 25 May 2018.

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently.

It is important to use this checklist and other Information Commissioner's Office (ICO) resources to work out the main differences between the current law and the GDPR. The ICO is producing new guidance and other tools to assist you, as well as contributing to guidance that the Article 29 Working Party is producing at the European level. These are all available via the ICO's [Overview of the General Data Protection Regulation](#). The ICO is also working closely with trade associations and bodies representing the various sectors – you should also work closely with these bodies to share knowledge about implementation in your sector.

It is essential to plan your approach to GDPR compliance now and to gain 'buy in' from key people in your organisation. You may need, for example, to put new procedures in place to deal with the GDPR's new transparency and individuals' rights provisions. In a large or complex business this could have significant budgetary, IT, personnel, governance and communications implications.

The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance with all the areas listed in this document will require organisations to review their approach to governance and how they manage data protection as a corporate issue. One aspect of this might be to review the contracts and other arrangements you have in place when sharing data with other organisations.

Some parts of the GDPR will have more of an impact on some organisations than on others (for example, the provisions relating to profiling or children's data), so it would be useful to map out which parts of the GDPR will have the greatest impact on your business model and give those areas due prominence in your planning process.

# 1

## Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one.

Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. You may find compliance difficult if you leave your preparations until the last minute.

# 2

## Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas.

The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

# 3

## Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to



complain to the ICO if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

The ICO's [Privacy notices code of practice](#) reflects the new requirements of the GDPR.

## 4

### Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

The right to data portability is new. It only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a structured commonly used and machine readable form and provide the

information free of charge.

## 5 Subject access requests

You should update your procedures and plan how you will handle requests to take account of the new rules:

- In most cases you will not be able to charge for complying with a request.
- You will have a month to comply, rather than the current 40 days.
- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

## 6 Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities you carry out and to identify your lawful basis for doing so. You should document your lawful bases in order to

help you comply with the GDPR's 'accountability' requirements.

## 7

### Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

You should read the [detailed guidance](#) the ICO has published on consent under the GDPR, and use our consent checklist to review your practices. Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Public authorities and employers will need to take particular care. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data.

You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

## 8

### Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services ('information society services') to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'.

This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

## 9

### Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

## 10

### Data Protection by Design and Data Protection Impact Assessments

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

You should therefore start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?

You should also familiarise yourself now with the [guidance the ICO has produced on PIAs](#) as well as [guidance from the Article 29 Working Party](#), and work out how to implement them in your organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management.

## 11

## Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

You should consider whether you are required to formally designate a Data Protection Officer (DPO). You must designate a DPO if you are:

- a public authority (except for courts acting in their judicial capacity);
- an organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
- an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions. The Article 29 Working Party has [produced guidance for organisations on the designation, position and tasks of DPOs](#).

It is most important that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.

12

## International

If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this.

The lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented.

This is only relevant where you carry out cross-border processing – ie you have establishments in more than one EU member state or you have a single establishment in the EU that carries out processing which substantially affects individuals in other EU states.

If this applies to your organisation, you should map out where your organisation makes its most significant decisions about its processing activities. This will help to determine your 'main establishment' and therefore your lead supervisory authority.

The Article 29 Working party has produced [guidance on identifying a controller or processor's lead supervisory authority](#).