

Your World First

C/M/S/

Law.Tax

# Towards GDPR compliance

Your Action Plan



2017 – 2018

## Contents

- 03 GDPR – are you ready for action?
- 04 GDPR Regulatory Risk Gauge
- 06 CMS GDPR Solutions
- 12 Breach Assistant
- 14 GDPR Action Plan

## Glossary

**BCRs** = Binding corporate rules

**DPA** = Data protection authority or supervisory authority

**DPIA** = Data protection impact assessment (currently, 'privacy impact assessments' or 'PIAs')

**DPO** = Data protection officer

**GDPR** = Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)



# GDPR – are you ready for action?

The General Data Protection Regulation (GDPR), which applies from 25 May 2018, will bring about a step change in risk for organisations that process personal data. Will your organisation be ready to comply from day one? It's time to take action.

You will have by now heard about the significant administrative fines that organisations may face for breaching the GDPR – depending on the type of breach, you could be looking at handing over up to the higher of:

- €20 million or 4% of the total worldwide annual turnover in the preceding financial year, or
- €10 million or 2% of the total worldwide annual turnover in the preceding financial year.

This considerably increases organisations' regulatory risk exposure to levels that demand proper attention.

The GDPR will also require extensive changes to be made to your organisation's operations and, in some cases, business models. Notably, the GDPR's wider scope captures certain processing operations outside the EEA and a broader range of processing activities, and the new 'accountability' principle will make developing a compliance culture a necessity rather than a 'nice to have'.

Further, there are the business risks associated with the costs of compliance with the enhanced obligations for both controllers and processors, and the wider impact of personal data breaches, to consider.

## Where do you start? Where should you focus your attention?

This Brochure is a highly practical guide to GDPR compliance, which includes:

- the '**GDPR Regulatory Risk Gauge**' (page 4-5) – this provides an indicative view of the key areas of exposure for organisations based on the level of regulatory risk
- '**CMS GDPR Solutions**' (pages 6-11) – this features some of CMS's pragmatic solutions designed to assist your organisation in achieving GDPR compliance
- '**CMS Breach Assistant**' (pages 12-13) – read about CMS's innovative online solution to assist organisations in dealing with data breaches, and
- the '**GDPR Action Plan**' (page 14 onwards) – this includes a list of 99 key actions to help your organisation work towards GDPR implementation.

This Brochure is not intended to be a definitive list of all your organisation's obligations under the GDPR, and different types of businesses will of course have different risk profiles. However, it aims to provide a useful focal point for discussions with key stakeholders in your organisation and to activate your GDPR implementation programme.

CMS's Data Protection team is also always on hand to provide commercially-focused advice on understanding and addressing your GDPR obligations in the context of your organisation.

For more information on the GDPR and what action you need to take, please contact **Emma Burnett**.



**Emma Burnett**

Partner, Head of Data Protection

T +44 20 7367 3565

E [emma.burnett@cms-cmck.com](mailto:emma.burnett@cms-cmck.com)

# GDPR Regulatory Risk Gauge





**How much is it going to cost us if we don't comply?** – is the question many organisations ask. Regulatory fines strike hard at a business' bottom line and the fact that the regulator has taken enforcement action can harm customers' and business partners' confidence in doing business with your organisation. This graphic summarises the key GDPR requirements by compliance area and the level of administrative fine applicable to infringement of that requirement: although there are obviously other risk areas and costs to business of non-compliance with data protection laws, this gives an indicative view of where your organisation might decide to focus its compliance efforts based on the level of regulatory risk.

# CMS GDPR Solutions

CMS can help you design and implement a range of pragmatic compliance solutions to support you in your objective of being a privacy-accountable organisation. Get the process started with our **CMS GDPR Action Plan** on page 14, then come and see us when you are ready to forge ahead.

Back this up with on-point expert advice. Rely on CMS's extensive expertise in data protection compliance projects across a range on industry sectors to enable your organisation to hit the ground running when the GDPR takes effect. For example, we can advise on which processing operations and activities are caught by the GDPR's wider scope, which regulators you will need to deal with, and when you need a data protection officer or a local representative, so that you can organise your business operations and governance structures effectively.

## How CMS can help

Our solutions are mapped against the GDPR requirements that need to be addressed in order to avoid Tier 1 and Tier 2 breaches, as summarised on the previous pages.



### Immediate priority

#### CMS GDPR Gap Analysis tools

Assess your organisation's current practices against what the GDPR requires and formulate a compliance action plan.

#### *GDPR requirements addressed:*

All, including Accountability and Governance.

#### Audit tools, project planning and data mapping guidance

Give your data processing activities a compliance health check; scope, project plan and prioritise; and consider how best to map data flows relevant to your organisation.

#### *GDPR requirements addressed:*

All, including Accountability and Governance.



### **Memoranda to the Board regarding data protection compliance**

Ensure that GDPR compliance receives due priority at board level and that key decisions are recorded for accountability purposes, eg a general memorandum on how to comply.

#### *GDPR requirements addressed:*

All, including Accountability and Governance.

### **CMS Lawful processing matrix**

Assess which legal bases for processing are valid and the most appropriate for your organisation to rely on.

#### *GDPR requirements addressed:*

Accountability and Governance, Processing Requirements (including consent generally), Data Subject Rights, Children's consent.

### **Representatives agreements**

Put in place effective contract documentation for the appointment of representatives by non-EU organisations.

#### *GDPR requirements addressed:*

Accountability and Governance, Enforcement Action and Supervisory Authority, Data Subject Rights, Processing Records.

### **DPO job specifications/ employment contracts** **Service contracts with outsourced/ external DPOs** **Internal DPO protocols**

Ensure your DPO is properly appointed and empowered to perform their tasks effectively, and that people in your organisation know what the DPO's function is and when and how to engage with them (including for DPIAs).

#### *GDPR requirements addressed:*

Accountability and Governance, Enforcement Action and Supervisory Authority, Data Subject Rights, Security and Data Breaches, DPIAs, Processing Records.



## Next priority

### Information notices and consents + checklist

Ensure the privacy information you provide to individuals is GDPR-compliant and the consents you obtain are valid.

#### *GDPR requirements addressed:*

Accountability and Governance, Processing Requirements (including consent generally), Data Subject Rights, International Transfers, Processors/Processing, Children's consent, Data Protection by Design and Default.

### Data subject rights forms

Facilitate the exercise by data subjects of their rights under the GDPR and ensure you receive the information you need to be able to respond effectively and within the required timescales.

#### *GDPR requirements addressed:*

Accountability and Governance, Processing Requirements, Data Subject Rights, Children's consent, Data Protection by Design and Default.

### Processor audit questionnaires

#### Data processing clauses/ agreements

#### Data protection clauses (GDPR) checklist

Use our audit questionnaires to do pre-contract due diligence on prospective processors. Put in place GDPR-compliant data processing contracts to protect your organisation when engaging processors or acting as a processor.

#### *GDPR requirements addressed:*

Accountability and Governance, Processing Requirements, Enforcement Action and Supervisory Authority, Data Subject Rights, International Transfers, Processors/Processing, Security and Data Breaches, Processing Records.

### DPIA toolkit:

- Preliminary assessment
- DPIA
- DPIA report

Use our DPIA tools to undertake DPIAs and implement the results of these into your organisation's projects, practices and procedures.

#### *GDPR requirements addressed:*

Accountability and Governance, Processing Requirements, Enforcement Action and Supervisory Authority, Data Subject Rights, International Transfers, Security and Data Breaches, Data Protection by Design and Default + DPIAs.



### **Privacy by design and default – developers' guidance**

Ensure technical teams are well versed in data protection by design and default principles so that new products and services have privacy 'built in'.  
*(Start earlier for high risk processing activities or new product launches)*

#### **GDPR requirements addressed:**

Accountability and Governance, Processing Requirements, Enforcement Action and Supervisory Authority, Data Subject Rights, International Transfers, Security and Data Breaches, Data Protection by Design and Default + DPIAs.

### **Data sharing agreements**

Put in place effective contract documentation for sharing personal data with other organisations as a controller.

#### **GDPR requirements addressed:**

Accountability and Governance, Processing Requirements, Enforcement Action and Supervisory Authority, Data Subject Rights, International Transfers, Supervisory Authority, Security and Data Breaches, Processing Records.

### **Internal data protection policies**

Have clear and workable internal policies addressing compliance with the extensive GDPR requirements applying to personal data processing, and that you can point to for accountability purposes.

#### **GDPR requirements addressed:**

All, including Accountability and Governance.

### **Information security (IS) policies**

Have clear and workable policies governing various aspects of information security, addressing the GDPR security requirements, and that you can point to for accountability purposes.

#### **GDPR requirements addressed:**

Accountability and Governance, Processing Requirements, International Transfers, Processors/Processing, Security and Data Breaches, Data Protection by Design and Default + DPIAs, Processing Records.



## By GDPR Day 1

### Assistance with obtaining certifications

Get support in obtaining certifications and advice on ongoing compliance with these from CMS's experienced Data Protection team.

#### *GDPR requirements addressed:*

All, including Accountability and Governance, Processing Requirements and International Transfers.

### Data processing records templates

Keep GDPR-compliant records of your organisation's data processing activities that record the data your organisation holds and uses so that this can be managed properly and also commercialised effectively.

#### *GDPR requirements addressed:*

Accountability and Governance, Processing Requirements, Enforcement Action and Supervisory Authority, Data Subject Rights, International Transfers, Processors/Processing, Security and Data Breaches, Processing Records.



## Ongoing

### Data transfer agreements

#### Binding corporate rules (BCRs)

#### EU-US Privacy Shield applications

Put in place effective mechanisms for transferring personal data internationally, such as data transfer agreements based on EU model clauses, BCRs and/ or Privacy Shield certification (but keep under review in light of new transfer mechanisms under the GDPR, plus ongoing court challenges and Brexit ramifications).

#### *GDPR requirements addressed:*

Accountability and Governance, Processing Requirements, Enforcement Action and Supervisory Authority, Data Subject Rights, International Transfers, Processors/Processing, Security and Data Breaches, Data Protection by Design and Default + DPIAs, Processing Records.

### Data governance frameworks

Put in place organisational structures and agreed principles for responsible and effective data governance to ensure your information assets and the associated risks are well-managed.

#### *GDPR requirements addressed:*

All, including Accountability and Governance.

### Privacy risks registers

Record the key privacy risks your organisation faces and formulate a plan to mitigate these.

#### *GDPR requirements addressed:*

All, including Accountability and Governance, Security and Data Breaches and DPIAs.

### CMS Breach Assistant (coming soon)

Access our CMS Breach Assistant microsite and app for a range of online ready resources all in one place to assist you in planning for and responding to a data breach rapidly and effectively (see page 12 for further information).

#### *GDPR requirements addressed:*

Accountability and Governance, Processing Requirements, Enforcement Action and Supervisory Authority, Processors/Processing, Security and Data Breaches.

### Cyber breach response support

Rely on CMS for urgent support with any data breaches, including with our 'best in class' cyber policy support product, coordinating legal support across multiple jurisdictions in the EMEA and beyond. As part of this, our data protection experts provide 24/7 counselling, investigations assistance, risk reports and legal and practical guidance in the critical period from cyber breach. We also provide expert assistance with notifications to regulators, data subjects and affected third parties.

#### *GDPR requirements addressed:*

Accountability and Governance, Processing Requirements, Enforcement Action and Supervisory Authority, Processors/Processing, Security and Data Breaches.

### Assistance in dealing with regulators

Get support from our experienced Data Protection team in dealing with DPAs (and other regulators) in matters such as enforcement action, prior consultation and approval of BCRs.

#### *GDPR requirements addressed:*

Enforcement Action and Supervisory Authority, Data Subject Rights, International Transfers, Security and Data Breaches, Data Protection by Design and Default + DPIAs.

### Training – bespoke training and CMS e-Learning (coming soon)

Train your staff on GDPR compliance across the various business functions that come into contact with personal data to ensure that your organisation can fulfil its obligations in practice.

#### *GDPR requirements addressed:*

All, including Accountability and Governance.

# Breach Assistant

## CMS Breach Assistant

Assistance at your fingertips in the event of a data breach.

The cost to business of a data breach, and the consequences for individuals whose data is compromised, can be extremely serious. **Do you know what to do in the event of a data breach?**

Time is critical when dealing with a data breach – the GDPR imposes formal personal data breach notification obligations, as do certain industry-specific regulations.

Organisations that do not comply face eye-watering fines (of up to the greater of €10 million or 2% of the total worldwide annual turnover) and other enforcement action for non-compliance with the GDPR notification requirements. This is in addition to the wide range of other potential exposures, such as reputational/ brand damage, loss of business, business interruption, forensic investigator costs and dealing with cyber extortion ransom demands...

CMS Breach Assistant provides a range of ready resources all in one place to assist you in planning for and responding to a data breach rapidly and effectively, including:

- Reference material that sets out the legal obligations your organisation needs to comply with
- Practical step by step guides about when to notify regulators, affected individuals and others
- The ability to personalise CMS Breach Assistant with contact information for your organisation's data breach response team
- Desktop and Mobile versions

Use CMS Breach Assistant to quickly mobilise your data breach response team and have to hand the information you need to be able to respond effectively.

Ask your CMS Data Protection team contact for further information.



## Breach Response

# My Information

Your data breach response team key contacts

CMS Data breach response team	
[Name], [Your Head of Information Security]	Email: [email@yourcompany.com] Mobile: [XXX]
[Name], [Your Data Protection Officer]	Email: [email@yourcompany.com] Mobile: [XXX]
[Name], [Your Head of Legal]	Email: [email@yourcompany.com] Mobile: [XXX]
[Name], [Your Head of Risk & Compliance]	Email: [email@yourcompany.com] Mobile: [XXX]



C/M'S/ Law. Tax Your World First


## Breach Assistant

Breach Assistant  
Assistance at your fingertips in the event of a data breach

# CMS Breach Assistant

Assistance at your fingertips in the event of a data breach

The GDPR defines a **"personal data breach"** as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".



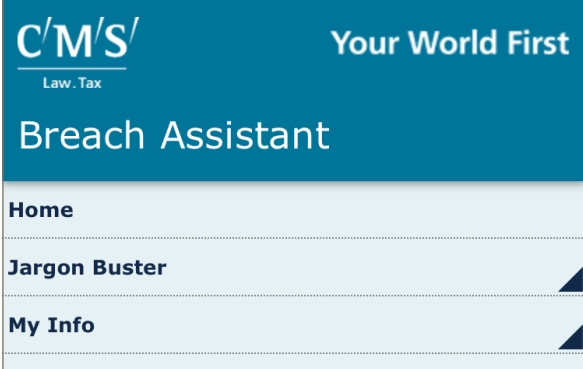
C/M'S/ Law. Tax Your World First

## Breach Assistant

Breach Assistant  
Assistance at your fingertips in the event of a data breach

Home > Breach Response

- Data breach response checklist
- Data breach plan
- Data breach report
- Post-breach action plan



C/M'S/ Law. Tax Your World First

## Breach Assistant

- Home
- Jargon Buster
- My Info
- Exposures
- Legal Framework
- Notify?

### NOTIFY?

- Notify regulators
- Communicating with individuals
- Contractual notifications requirements



# GDPR Action Plan

So, you know about the risks. Now, it's time to take action.

GDPR compliance is much more than just a tick box exercise - but a checklist is always a good place to start when faced with an epic implementation task.

The **99 point action plan** included in this Brochure contains a more detailed summary of the GDPR requirements relevant to each of the Tier 1 and Tier 2 breaches, together with a non-exhaustive list of key compliance actions, which you can tick off as your organisation works through its GDPR implementation programme. The action plan is designed to form the basis for a more detailed gap analysis between your organisation's current practices and processes and the increased requirements under the GDPR.

## Notes:

The action plan only covers the obligations of controllers and processors and does not cover the obligations of other persons subject to regulation under the GDPR, ie certification bodies (Article 43) or accredited compliance bodies (Article 41(4))

Member States may impose rules on criminal sanctions for infringements of the GDPR too and may also allow for the deprivation of the profits gained from non-compliance with the GDPR. However, this action would be instead of, not in addition to, any administrative fine or other penalty (Recital 149)





## Data Protection contacts

### John Armstrong

E [john.armstrong@cms-cmck.com](mailto:john.armstrong@cms-cmck.com)  
T +44 20 7367 2701

### Emma Burnett

E [emma.burnett@cms-cmck.com](mailto:emma.burnett@cms-cmck.com)  
T +44 20 7367 3565

### Alan Nelson

E [alan.nelson@cms-cmck.com](mailto:alan.nelson@cms-cmck.com)  
T +44 141 304 6006

### Tom Scourfield

E [tom.scourfield@cms-cmck.com](mailto:tom.scourfield@cms-cmck.com)  
T +44 20 7367 2707

### Ian Stevens

E [ian.stevens@cms-cmck.com](mailto:ian.stevens@cms-cmck.com)  
T +44 20 7367 2597

### Loretta Pugh

E [loretta.pugh@cms-cmck.com](mailto:loretta.pugh@cms-cmck.com)  
T +44 20 7367 2730

### Duncan Turner

E [duncan.turner@cms-cmck.com](mailto:duncan.turner@cms-cmck.com)  
T +44 131 200 7669

## Employment contacts

### Sarah Ozanne

E [sarah.ozanne@cms-cmck.com](mailto:sarah.ozanne@cms-cmck.com)  
T +44 20 7367 2650

### Graham Paul

E [graham.paul@cms-cmck.com](mailto:graham.paul@cms-cmck.com)  
T +44 20 7367 2458

### Alison Woods

E [alison.woods@cms-cmck.com](mailto:alison.woods@cms-cmck.com)  
T +44 122 426 7176





Law. Tax

**Your free online legal information service.**

A subscription service for legal articles on a variety of topics delivered by email.

**[cms-lawnow.com](http://cms-lawnow.com)**



Law. Tax

**Your expert legal publications online.**

In-depth international legal research and insights that can be personalised.

**[eguides.cmslegal.com](http://eguides.cmslegal.com)**

-----

CMS Legal Services EEIG (CMS EEIG) is a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices.

**CMS locations:**

Aberdeen, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Kyiv, Leipzig, Lima, Lisbon, Ljubljana, London, Luxembourg, Lyon, Madrid, Medellín, Mexico City, Milan, Moscow, Munich, Muscat, Paris, Podgorica, Prague, Rio de Janeiro, Rome, Santiago de Chile, Sarajevo, Seville, Shanghai, Sofia, Strasbourg, Stuttgart, Tehran, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

-----

**[cms.law](http://cms.law)**