

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

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 of 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".



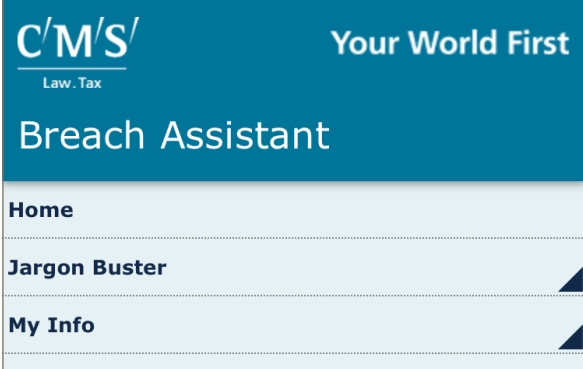
C'M/S/ Law. Tax Your World First

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)



CMS GDPR Action Plan

Tier 1 Breaches – €20m/4% of worldwide annual turnover

Processing requirements				
Requirement	GDPR provision	Person responsible	Action	
Failure to comply with the principles relating to processing of personal data: — lawfulness, fairness and transparency — purpose limitation — data minimisation — accuracy — storage limitation — integrity and confidentiality (security) — accountability Note: <i>The transparency/ fair processing information that needs to be provided under the GDPR is much more detailed than currently is the case.</i>	Article 5	Controller	1. Update your information notices to include the required additional transparency/fair processing information to individuals 2. Update your data collection, data handling, security and data retention practices and policies to ensure compliance with the revised data protection principles 3. Require contractual assurances that any bought-in data lists are legally compliant with GDPR requirements – eg, check upstream and downstream permissions for linkage/ matched data 4. Use pseudonymisation/ anonymisation and encryption, where appropriate 5. Implement and maintain appropriate technical and organisational security measures (ie access controls and technical safeguards) and conduct regular security testing and keep testing records 6. Keep documentary evidence to demonstrate compliance with the data protection principles for accountability purposes (eg processing records, data mapping, data governance frameworks, DPIAs) 7. Train relevant staff on data protection compliance best practice and keep training records	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Failure to comply with the conditions relating to lawful processing Note: <i>The requirements for valid consent under the GDPR are much more detailed than is currently the case.</i>	Article 6	Controller	8. Review your legal bases for processing to ensure these remain lawful and appropriate, in particular regarding consent 9. Update information notices and consents to state the legal bases on which personal data is being processed 10. Conduct periodic reviews of the effectiveness and accuracy of policies/procedures regarding secondary uses of personal data to ensure this is only used for compatible purposes 11. Monitor for Member State laws relating to processing that is necessary for compliance with a legal obligation or for performance of a task carried out in the public interest/exercise of official authority	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Failure to comply with the conditions for consent	Article 7	Controller	12. Update your consents to comply with the stricter requirements for valid consent (eg, ‘re-permission’ in advance to allow time for individuals to respond)	<input type="checkbox"/>
Failure to comply with requirements for processing special categories of personal data	Article 9	Controller	13. Ensure any processing of sensitive/special categories of personal data: (a) comes within an exemption to the general prohibition on processing these categories of data in Article 9, and (b) has a legal basis (under Article 6) as well – see above 14. Update your consents to comply with the stricter requirements for ‘explicit’ consent	<input type="checkbox"/> <input type="checkbox"/>
Data subject rights				
Requirement	GDPR provision	Person responsible	Action	
Failure to give effect to certain rights of data subjects: — information and access — rectification and erasure — restriction and data portability — objection and automated decision-making	Articles 12-22	Controller	15. Update your information notices to include the required additional transparency/fair processing information, including regarding data subject rights 16. Ensure your systems are set up to deal with the enhanced data subject rights (eg, 30-day response time, data portability, processes for notifying other data recipients of erasure and restriction requests) 17. Ensure that processors are contractually obliged to pass on data subject requests and provide assistance with these 18. Train relevant staff on responding to data subject requests, and keep training records	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
International transfers				
Requirement	GDPR provision	Person responsible	Action	
Transfer of personal data to third countries or international organisations without ensuring an adequate level of protection or applying an exemption	Articles 44-49	Controller/ Processor	19. Put in place appropriate data transfer agreements including EU Model Clauses, BCRs or other approved mechanisms 20. Review derogations relied on to ensure these remain lawful and appropriate, in particular regarding consent 21. Ensure processor/sub-processor contracts include protections against unauthorised transfers/onward transfers	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Specific processing situations				
Requirement	GDPR provision	Person responsible	Action	
Failure to comply with Member State laws for specific processing	Chapter IX	Controller	22. Monitor for Member State laws relating to specific processing situations (ie, freedom of expression; employment; public access to official documents; archiving in the public interest, scientific/ historical research or statistics; and secrecy) 23. TBC – awaiting enactment of relevant Member State laws and DPA guidance	<input type="checkbox"/> <input type="checkbox"/>
Enforcement action				
Requirement	GDPR provision	Person responsible	Action	
Non-compliance with supervisory authority corrective/ investigative powers	Article 58	Controller/ Processor	24. Implement and maintain effective data governance processes 25. Ensure processors/subcontractors are contractually obliged to refer any notices from DPAs 26. Train relevant staff on data protection compliance best practice and dealing with regulators, and keep training records	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Tier 2 Breaches – €10m/2% of worldwide annual turnover

Requirement	GDPR provision	Person responsible	Action	
Failure by non EU controllers to designate appropriate representatives in the EU	Article 27	Controller	27. If required, duly appoint a representative	<input type="checkbox"/>
			28. Enter into representative agreement(s) that set out your representative's appointment and obligations	<input type="checkbox"/>
			29. Provide information about your representative(s) to data subjects and the DPA(s)	<input type="checkbox"/>
			30. Consider carefully whether or not to act as representative for another entity	<input type="checkbox"/>
Failure by non EU processors to designate appropriate representatives in the EU	Article 27	Processor	31. If required, duly appoint a representative	<input type="checkbox"/>
			32. Enter into representative agreement(s) that set out your representative's appointment and obligations	<input type="checkbox"/>
			33. Provide information about your representative(s) to data subjects and the DPA(s)	<input type="checkbox"/>
			34. Consider carefully whether or not to act as representative for another entity	<input type="checkbox"/>
Data Protection Officer ('DPO')				
Requirement	GDPR provision	Person responsible	Action	
Failure by a controller to appropriately appoint a DPO where required	Articles 37-39	Controller	35. If required, appoint a DPO	<input type="checkbox"/>
			36. Ensure the DPO is properly appointed in terms of mandate, position in the organisation, confidentiality and resources	<input type="checkbox"/>
			37. Ensure that internal governance processes require the DPO to be involved in data protection issues	<input type="checkbox"/>
			38. Provide information about your DPO to the supervisory authority(s) and on your website	<input type="checkbox"/>
Failure by a processor to appropriately appoint a DPO where required	Articles 37-39	Processor	39. If required, appoint a DPO	<input type="checkbox"/>
			40. Ensure the DPO is properly appointed in terms of mandate, position in the organisation, confidentiality and resources	<input type="checkbox"/>
			41. Ensure that internal governance processes require the DPO to be involved in data protection issues	<input type="checkbox"/>
			42. Provide information about your DPO to the DPA(s) and on your website	<input type="checkbox"/>
Security				
Requirement	GDPR provision	Person responsible	Action	
Failure by controllers to implement appropriate technical and organisational measures	Article 32	Controller	43. Implement and maintain appropriate technical and organisational security measures, ie: <ul style="list-style-type: none">• physical and personnel access controls• encryption and pseudonymisation/anonymisation• IS policies and procedures and data breach response plans	<input type="checkbox"/>
			44. Comply with any approved codes of conduct or certification mechanisms regarding security	<input type="checkbox"/>
			45. Conduct regular compliance checks to verify the effectiveness of such measures (including resilience/ penetration testing), particularly if there has been a data breach, and keep testing records	<input type="checkbox"/>
Failure by processors to implement appropriate technical and organisational measures	Article 32	Processor	46. Implement and maintain appropriate technical and organisational security measures, ie: <ul style="list-style-type: none">• physical and personnel access controls• encryption and pseudonymisation/anonymisation• IS policies and procedures and data breach response plans	<input type="checkbox"/>
			47. Comply with any approved codes of conduct or certification mechanisms regarding security	<input type="checkbox"/>
			48. Conduct regular compliance checks to verify the effectiveness of such measures (including resilience/ penetration testing), particularly if there has been a data breach, and keep testing records	<input type="checkbox"/>
Personal data breaches				
Requirement	GDPR provision	Person responsible	Action	
Failures in relation to notification of a personal data breach to the supervisory authority	Article 33	Controller	49. Implement processes and procedures to ensure personal data breaches are notified to the DPA within 72 hours of knowing of breach (eg, early warning flags, data governance frameworks, data breach response plans)	<input type="checkbox"/>
			50. Document all personal data breaches, including the relevant facts, effects and remedial action	<input type="checkbox"/>
			51. Ensure your processor contracts require processors to inform you of data breaches promptly so you can notify the DPA in time	<input type="checkbox"/>
Failures in relation to communication of a personal data breach to data subjects	Article 34	Controller	52. Implement processes and procedures to ensure personal data breaches are communicated to affected data subjects promptly where required/ appropriate (eg data governance frameworks and data breach response plans)	<input type="checkbox"/>
			53. Ensure technical measures such as encryption are used, where appropriate	<input type="checkbox"/>
			54. Ensure any orders by the DPA to communicate data breaches to affected data subjects are complied with	<input type="checkbox"/>
			55. Ensure your processor contracts require processors to inform you of data breaches promptly so you can communicate the breach to affected data subjects without delay, if appropriate	<input type="checkbox"/>
Data processors				
Requirement	GDPR provision	Person responsible	Action	
Failure by controllers to only use processors who provide sufficient guarantees to implement appropriate technical and organisational measures	Article 28(1)	Controller	56. Carry out comprehensive due diligence/ audits to ensure you only engage processors that maintain appropriate security processes and standards	<input type="checkbox"/>
			57. Put in place processing contracts that oblige processors to implement appropriate technical and organisational measures (including regarding security and transfers)	<input type="checkbox"/>
Subcontracting of processing by processors without controller authorisation	Article 28(2)	Processor	58. Ensure restrictions on subcontracting processing without controller authorisation in processing contracts are complied with	<input type="checkbox"/>
Non-compliance with the requirement to have a processing contains certain details	Articles 28(3)-(9)	Controller	59. Put in place processing contracts that contains all of the required details, including: <ul style="list-style-type: none">• that personal data is processed only on the controller's documented instructions• standard contractual clauses approved by the DPA (if any)• allocating liability appropriately	<input type="checkbox"/>
			60. Exercise audit and inspection rights to verify compliance by processors with their obligations	<input type="checkbox"/>
Failure of processors to only process personal data on the controller's instructions	Article 29	Processor	61. Put in place processing contracts that comprehensively set out the controller's instructions (including regarding transfers); include cost and liability protections	<input type="checkbox"/>
			62. Maintain internal data handling, security and data retention practices and policies to ensure compliance with the controller's instructions	
			63. Train relevant staff on data handling best practice and ensure processing is not excessive, and keep training records	
Data Protection Impact Assessments ('DPIAs') and Supervisory Authority consultations				
Requirement	GDPR provision	Person responsible	Action	
Failures by a controller in relation to DPIAs	Article 35	Controller	64. Train technical teams/developers about privacy by design and by default, and keep training records	<input type="checkbox"/>
			65. Implement technical and organisational measures to ensure data protection by design and by default	<input type="checkbox"/>
			66. Carry out DPIAs for new or updated processing and projects (and reviews where there is a change in risk), where required, seeking the DPO's advice	<input type="checkbox"/>
			67. Comply with any approved codes of conduct or lists of processing activities relevant to DPIAs and, where appropriate, seek data subject input	<input type="checkbox"/>
Failures by a controller to, where necessary, consult with the supervisory authority prior to high risk processing	Article 36	Controller	68. Consult with DPAs if a DPIA concludes that processing is high risk	<input type="checkbox"/>
			69. Implement the DPA's recommendations (eg by updating processes and procedures, implementing additional protections)	<input type="checkbox"/>
			70. Train relevant staff on dealing with DPAs, and keep training records	<input type="checkbox"/>
Data protection by design and by default				
Requirement	GDPR provision	Person responsible	Action	
Failure to implement technical and organisational measures to ensure data protection by design and by default	Article 25	Controller	71. Train technical teams/developers about privacy by design and by default, and keep training records	<input type="checkbox"/>
			72. Implement technical and organisational measures to ensure data protection by design/by default (eg, pseudonymisation, and to ensure data collection is not excessive and secure deletion of data when no longer needed for the specified purpose)	<input type="checkbox"/>
			73. Carry out DPIAs for new or updated processing and projects, particularly high risk processing	<input type="checkbox"/>
Records				
Requirement	GDPR provision	Person responsible	Action	
Failure of controllers to keep processing records	Article 30(1)	Controller	74. Carry out mapping of relevant data flows and processing activities	<input type="checkbox"/>
			75. Set up and maintain appropriate records of processing	<input type="checkbox"/>
			76. Ensure your processor contracts require processors to give you the information you need in order to comply	<input type="checkbox"/>
			77. Update records regularly to take into account changes to details such as representatives, DPOs, processing activities and security measures	<input type="checkbox"/>
Failure of processors to keep processing records	Article 30(2)	Processor	78. Carry out mapping of relevant data flows and processing activities	<input type="checkbox"/>
			79. Set up and maintain appropriate records of processing	<input type="checkbox"/>
			80. Ensure sub-processors give you the information you need in order to comply (eg include obligations in processing contracts)	<input type="checkbox"/>
			81. Update records regularly to take into account changes to details such as representatives, DPOs, processing activities and security measures	<input type="checkbox"/>
Re-identification and data subject rights				
Requirement	GDPR provision	Person responsible	Action	
Failure to give effect to certain of a data subject's rights where the controller is able to identify the data subject (having been given the additional information to identify them)	Article 11	Controller	82. Update data collection, data handling, security and data retention practices and policies to ensure compliance with this requirement	<input type="checkbox"/>
			83. Ensure your systems are set up to deal with the enhanced data subject rights (eg 30-day response time, data portability, processes for notifying other data recipients of erasure and restriction requests)	<input type="checkbox"/>
			84. Train relevant staff on responding to data subject requests, and keep training records	<input type="checkbox"/>
Joint controllers				
Requirement	GDPR provision	Person responsible	Action	
Failure by joint controllers in being transparent about their respective compliance obligations	Article 26	Controller	85. Update information notices to include details about joint processors and designate a point of contact for data subject requests	<input type="checkbox"/>
			86. Enter into data sharing agreements setting out each controller's rights and responsibilities and the agreed process for dealing with data subject requests	<input type="checkbox"/>
Consent – children				
Requirement	GDPR provision	Person responsible	Action	
Failures in relation to consent for processing children's personal data	Article 8	Controller	87. Update your consents, age verification and authorisation processes to comply with the stricter requirements for valid consent for processing children's personal data	<input type="checkbox"/>
Certification				
Requirement	GDPR provision	Person responsible	Action	
Where a controller relies on certification for compliance but fails to comply with the relevant obligations	Article 42	Controller	88. Ensure all relevant requirements for maintaining certifications are complied with – TBC	<input type="checkbox"/>
			89. Conduct regular compliance checks to verify compliance with certification requirements – TBC	<input type="checkbox"/>
			90. Train relevant staff on relevant requirements for maintaining certification and data protection compliance best practice, and keep training records	<input type="checkbox"/>
Where a processor relies on certification for compliance but fails to comply with the relevant obligations	Article 42	Processor	91. Ensure all relevant requirements for maintaining certification are complied with	<input type="checkbox"/>
			92. Conduct regular compliance checks to verify compliance with certification requirements	<input type="checkbox"/>
			93. Train relevant staff on relevant requirements for maintaining certification and data protection compliance best practice, and keep training records	<input type="checkbox"/>
Supervisory authority				
Requirement	GDPR provision	Person responsible	Action	
Failure by controllers to cooperate with the supervisory authority	Article 31	Controller	94. Implement and maintain effective governance processes	<input type="checkbox"/>
			95. Ensure your processor contracts require processors to promptly pass on all DPA notices and communications and to give you the cooperation and assistance you need in order to comply	<input type="checkbox"/>
			96. Train relevant staff on data protection best practice and dealing with regulators, and keep training records	<input type="checkbox"/>
Failure by processors to cooperate with the supervisory authority	Article 31	Processor	97. Implement and maintain effective governance processes	<input type="checkbox"/>
			98. Ensure processor contracts require controllers and sub-processors to promptly pass on all DPA notices and communications and to give you the cooperation and assistance you need in order to comply	<input type="checkbox"/>
			99. Train relevant staff on data protection best practice and dealing with regulators, and keep training records	<input type="checkbox"/>

Data Protection contacts

John Armstrong

E john.armstrong@cms-cmck.com
T +44 20 7367 2701

Emma Burnett

E emma.burnett@cms-cmck.com
T +44 20 7367 3565

Alan Nelson

E alan.nelson@cms-cmck.com
T +44 141 304 6006

Tom Scourfield

E tom.scourfield@cms-cmck.com
T +44 20 7367 2707

Ian Stevens

E ian.stevens@cms-cmck.com
T +44 20 7367 2597

Loretta Pugh

E loretta.pugh@cms-cmck.com
T +44 20 7367 2730

Duncan Turner

E duncan.turner@cms-cmck.com
T +44 131 200 7669

Employment contacts

Sarah Ozanne

E sarah.ozanne@cms-cmck.com
T +44 20 7367 2650

Graham Paul

E graham.paul@cms-cmck.com
T +44 20 7367 2458

Alison Woods

E 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



Law. Tax

Your expert legal publications online.

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

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