DATA & INFORMATION CONTACTS



HELENA BROWN Partner

0131 222 9544 07407 735 118 helena.brown@addleshawgoddard.com



BEATRICE DUKE Managing Associate 0113 209 2019

07730 320881 beatrice.duke@addleshawgoddard.com

MARCUS TURLE

Consultant 07957 692794 marcus.turle@mj-legal.co.uk



JO SNEDDEN Associate

0131 222 9541 07501 463230 joanne.snedden@addleshawgoddard.com

CALUM FISHER Managing Associate

0141 574 2462 07436 583 178 calum.fisher@addleshawgoddard.com

CLAIRE COLQUHOUN Associate

0131 222 9875 07595 192567 claire.colquhoun@addleshawgoddard.com

Action Plan



addleshawgoddard.com

Aberdeen, Doha, Dubai, Edinburgh, Glasgow, Hong Kong, Leeds, London, Manchester, Muscat, Singapore and Tokyo*

* a formal alliance with Hashidate Law Office

© 2017 Addleshaw Goddard LLP. All rights reserved. Extracts may be copied with prior permission and provided their source is acknowledged. This document is for general information only. It is not legal advice and should not be acted or relied on as being so, accordingly Addleshaw Goddard disclaims any responsibility. It does not create a solicitor-client relationship between Addleshaw Goddard and any other person. Legal advice should be taken before applying any information in this document to any facts and circumstances. Addleshaw Goddard is an international legal practice carried on by Addleshaw Goddard by the Solicitors Regulation Authority and the Law Society of Scotland) and its affiliated undertakings. Addleshaw Goddard (GCC) LLP (icensed by the OFCA), in Oman through Addleshaw Goddard (Middle East) LLP in essociation with Nasser Al Habsi & Saif Al Mamari Law Firm (licensed by the Oman Ministry of Justice) and in Hong Kong, Addleshaw Goddard (Hong Kong) LLP, a Hong Kong limited liability partnership pursuant to the Legal Practitioners Ordinance and regulated by the Law Society of Hong Kong. In Tokyo, legal services are offered through Addleshaw Goddard were the use form alliance with Hashidate Law Office. A list of members/principals for each firm will be provided upon request. The term partner refers to any individual who is a member of any Addleshaw Goddard entity or association or an employee or consultant with equivalent standing and qualifications. If you prefer not to receive promotional material from us, please email us at unsubscribe@addleshaw Goddard or further information or an employee or consultant with equivalent standing and qualifications. If you prefer not to receive promotional material from us, please email us at unsubscribe@addleshaw Goddard or further information please consult our website www.addleshawgoddard.

REF:10644

ADDLESHAW GODDARD

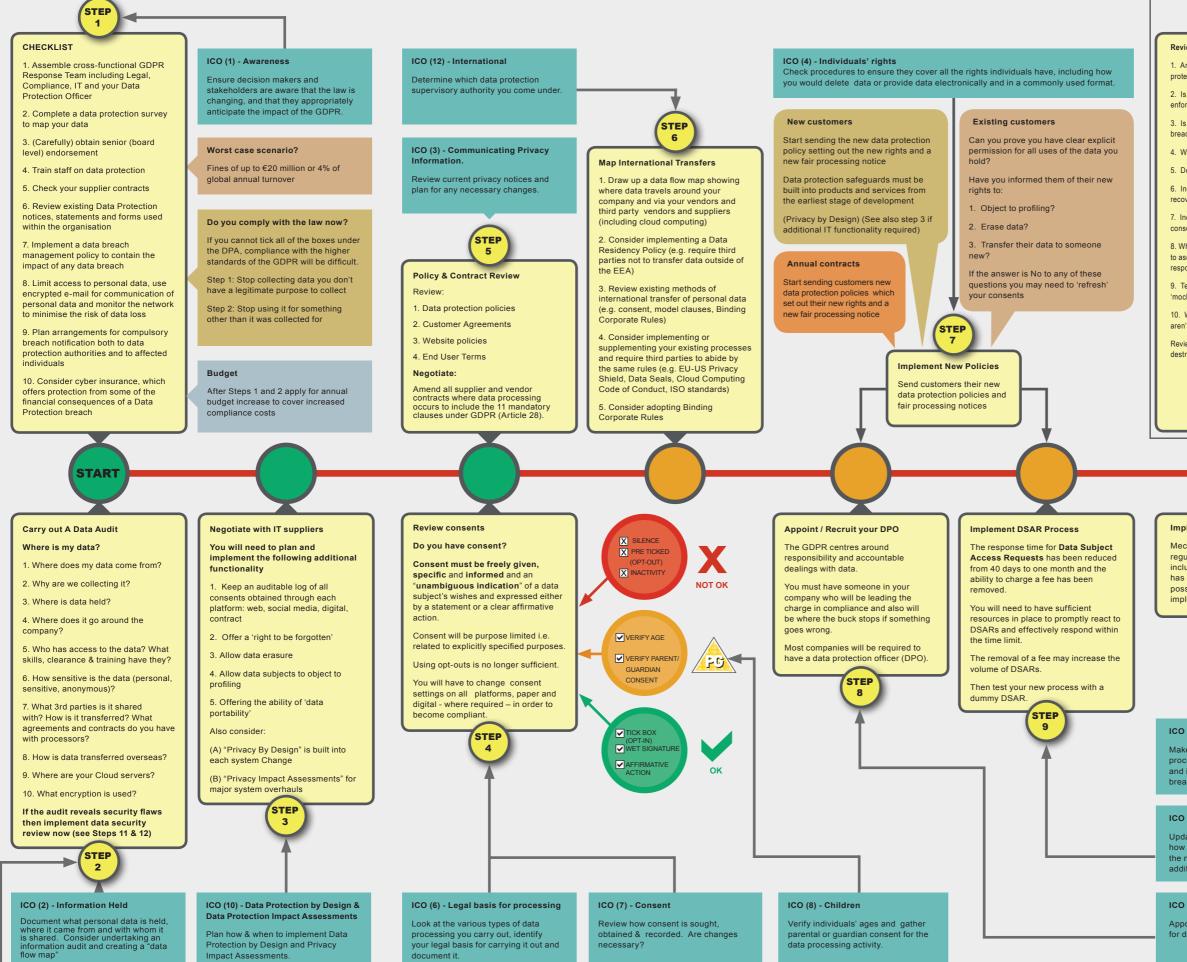
GENERAL DATA PROTECTION REGULATION (GDPR)

What to do and when to do it



ADDLESHAW GODDARD

OUR 12 STEP PLAN TO COMPLY WITH THE GENERAL DATA PROTECTION REGULATION



Accelerate these steps to earlier in the programme if the Data Audit in Step 2 identifies security flaws

(e.g. between Steps 2 and 3)



Review your data security

1. Are there adequate firewalls and virus protections?

STEP

11

2. Is there a clear password policy? Is it enforced?

3. Is there a procedure in place for data breach management?

4. Who is responsible for it?

5. Do all staff understand the procedure?

6. Include response, notification process recovery and damage limitation

7. Include risk assessment for the consequences of the breach?

8. What investigative process is triggered to ascertain the cause of the breach and if response can be improved?

9. Test breach management procedure with a 'mock' breach?

10. What do you do with your data when you aren't using it?

Review storage and data elimination / destruction policies

Implement First 24 hrs Data Security Action Plan

1. Mobilise crisis management team with support from communications and legal advisers to begin executing your incident response plan

2. Record the date and time when the breach was discovered Alert and activate everyone on the response team, including external resources.

 Secure the IT systems to stop additional data loss. Take affected equipment offline but do not turn them off or start probing into the computer until your forensics team arrives

4. Document everything known thus far about the attack

5. Interview those involved in discovering the breach and anyone else who may know about it.

6. Review protocols regarding disseminating information about the breach.

7. Assess priorities and risks based on what you know about the breach

8. Bring in your forensics team to begin an in-depth investigation

 Protect your reputation with an internal and external communications strategy, supported as necessary by crisis communications specialists and/or reputation lawyers

10. Report to police, regulators, and insurance brokers after consulting with legal and upper management.lice, if/when considered appropriate

END

Implement Breach Reporting

Mechanisms to notify the national regulator of data breaches, including which individuals' data has been compromised as soon as possible (within 72 hours) should be implemented and tested.



ICO (9) - Data breaches

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

ICO (5) - Subject access requests

Update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

ICO (11) - Data Protection Officer

Appoint someone to take responsibility for data protection compliance.

Notes

The ICO has published a 12 step guidance on how to prepare for the GDPR.

We have overlaid the ICO 12 Steps against our own recommended preparation programme.

If you follow the steps 1 to 12 in the order suggested you will also comply with the ICO guidance.

Steps 11 & 12 relate to data security. If your data audit (Step 2) reveals security flaws you may wish to accelerate your data security review and implement the Data Security 24HR response plan to deal with data breaches (Steps 11 and 12).

For further information about our Data and Information team please contact:

Helena Brown Partner 0131 222 9544 07407 735 118 helena.brown@addleshawgoddard.com or Beatrice Duke Managing Associate 0113 209 2019 07730 320 881 beatrice.duke@addleshawgoddard.com