GDPR

CHEAT SHEET

A practical guide for
Chambers and Law Firms

WHITE PAPER BY

SPROUT IT
LEGAL IT SPECIALISTS

www.SproutIT.co.uk
AskTheExpert@SproutIT.co.uk
+44 (0) 20 70368530
@Sprout_IT
Sprout IT

ABOUT SPROUT IT

SproutIT enable law firms & barristers' chambers to achieve competitive advantage and peace of mind, through the innovative use of best-of-breed technology, focussed cyber security and resilience, award winning services, and passion for service excellence.

From Document Management Solutions and Fees/Diary software, to email archive, compliance, encryption and security, Sprout IT can plan, implement and support your entire infrastructure.

Preparing your legal practice for the General Data Protection Regulation

The GDPR is immediately enforceable from 25th May 2018. Whilst the GDPR is similar to the Data Protection Act, it is broader in scope, strengthens rights of the individual, and, of course, is backed by higher penalties.

Here, we will highlight the main areas for your attention, along with expert tips and an action plan.

Regulation

A regulation is a legal act of the European Union that becomes immediately enforceable as law in all member states simultaneously – it does not need to be transposed into National law.

Objective

The primary objectives of the GDPR are to give control back to citizens and residents over their personal data and to simplify the regulatory environment by unifying the regulation within the EU.

Brexit

Brexit or no Brexit, the GDPR is coming. Not only will it be in force long before Brexit may (or may not!) be completed, the Government and ICO have confirmed that we will continue to abide by the GDPR.

Example fines =
£120,000

Under GDPR
£4.3 Million

In October 2012 a solicitor in the uk sent an email to the wrong client and was fi ned £120,000 under the 1998 Act. Under the GDPR that fi ne is estimated to be £4.3 million.

GAP Analysis - The process

Sprout's Gap Analysis tool and consultancy services are based on 10 sections.
We will investigate, consult on and understand your positions regarding:

1. Governance
2. Risk management
3. GDPR project
4. Data Protection Officer
5. Roles & responsibilities
6. Scope of compliance
7. Process analysis
8. Personal Information Management System (PIMS)
9. Information Security Management System (ISMS)
10. Individual's rights

The GA process will help establish the next steps for compliance with the Regulation and to identify processes that involve personal data.

SPROUT IT
LEGAL IT SPECIALISTS

www.SproutIT.co.uk
AskTheExpert@SproutIT.co.uk
+44 (0) 20 70368530
@Sprout_IT
Sprout IT

GAP Analysis - The output

Your Gap Analysis will include these 12 areas, and will show the areas in which you're compliant as well as highlighting those which require closer attention.

1. Organisational awareness

Ensure your key decision makers are aware of the GDPR and the changes it brings. Look at, and maintain, your corporate Risk Register.

SPROUT TIP

Start now – decision makers don't like last minute surprises or budget requests.

2. Information you hold

Identify any personal data you hold, understand where it came from, and who you share it with – document the journey of that data in, through, and out of your organisation. You're accountable for this data under the GDPR, so start evidencing your compliance.

SPROUT TIP

Work through each department within your organisation. Consider how and where you use the information you collect. Audit how you store and track that information.

3. Communicating privacy

Review your Privacy Notices and be sure to include mandatory information. Publish as GDPR goes live.

SPROUT TIP

You must use clear and easy to understand language. Explain your lawful basis for processing their data and how long you will retain it.

4. Individual's rights

Individuals have very important rights within the GDPR – ensure you address them all, to: be informed, have access, rectification, erasure, restrict processing, portability, object.

SPROUT TIP

If you are compliant with the DPA already, then this transition could be straightforward. Check you have documented procedures and technologies in place to cover all rights.

5. Subject access request

You will need to handle requests from a data subject, under the new rules.

SPROUT TIP

You will have only 1 month (down from 40 days) to comply, and will not usually be able to charge for complying with a request. Consider how you would handle a large number of simultaneous requests.

6. Lawful basis for processing personal data

Identify the lawful basis for your processing activity, document it and update your privacy notice to explain it.

SPROUT TIP

The lawful bases in the GDPR are broadly the same conditions for processing in the DPA – but the implications are modified. Document everything to achieve 'accountability'.

SPROUT IT
LEGAL IT SPECIALISTS

www.SproutIT.co.uk
AskTheExpert@SproutIT.co.uk
+44 (0) 20 70368530
@Sprout_IT
Sprout IT

GAP Analysis - The output

7. Consent

Review and modify how you seek, record and manage consent. Consent cannot be inferred.

SPROUT TIP Refresh existing consents, in time for the GDPR.

8. Children

Consider whether you need to verify individuals' ages and to obtain parental/ guardian consent.

SPROUT TIP The GDPR sets the age when a child can give their own consent at 16. This may be lowered to 13, in the UK.

9. Data breaches

You must have the right technologies and procedures in place to detect, report and investigate a personal data breach.

SPROUT TIP Breach reporting is now mandatory and must be within 72 hours. Consider your whole breach process, to include reporting,

10. Data Protection by Design and Data Protection Impact Assessments (DPIA)

Previously good practice, the GDPR makes privacy-by-design an express legal requirement, under the term 'data protection by design and by default'.

SPROUT TIP Run a DPIA whenever you deploy new technology. Consider a DPIA on your existing systems, too.

11. Data Protection Officers (DPO)

Your DPO should report directly to the highest management level of your organisation. You may outsource this role.

SPROUT TIP Designate someone to take responsibility for data protection compliance; avoid confl icts of interest.

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.

SPROUT TIP Also consider what data you keep and where you keep it. Ensure 'adequacy' exists, in that country, either granted by the EU or via other controls such as the Privacy Shield.

For further information on GDPR call 020 7036 8530
or email iberhnardt@sproutit.co.uk

SPROUT IT
LEGAL IT SPECIALISTS

www.SproutIT.co.uk
AskTheExpert@SproutIT.co.uk
+44 (0) 20 70368530
@Sprout_IT
Sprout IT

To conclude

1. If you accept that brand awareness and reputation are key to the survival and growth of your practice, then you might also consider how to build reputational resilience in the form of a Cyber and GDPR strategy.

2. To be compliant, you must blend People, Process and Technology.
No single piece of technology will make you compliant – there is no silver bullet.

3. GDPR should not simply be a tick box exercise, but an opportunity to improve your business practice, mitigate risk and promote transparency.

With the end of the 'affordable data breach' and to defend reputational risk, we are developing smart ways to help you.

Call us now on 020 7036 8530

We're happy to have a confidential discussion, under NDA if you prefer.

We are qualified, experienced and trusted

We're ISO 17024-accredited EU GDPR Foundation (EU GDPR F) and EU GDPR Practitioner (EU GDPR P)

- We're accredited by the Institute of Information Security Professionals (IISP) -

Skills Framework Level 1: A1, A2, A3, A4, A5, A6, A7, B1 and C2

- We have 10+ years of practical data protection experience, blended with IT Strategy and Cyber Resilience expertise

SPROUT IT
LEGAL IT SPECIALISTS

www.SproutIT.co.uk
AskTheExpert@SproutIT.co.uk
+44 (0) 20 70368530
@Sprout_IT
Sprout IT