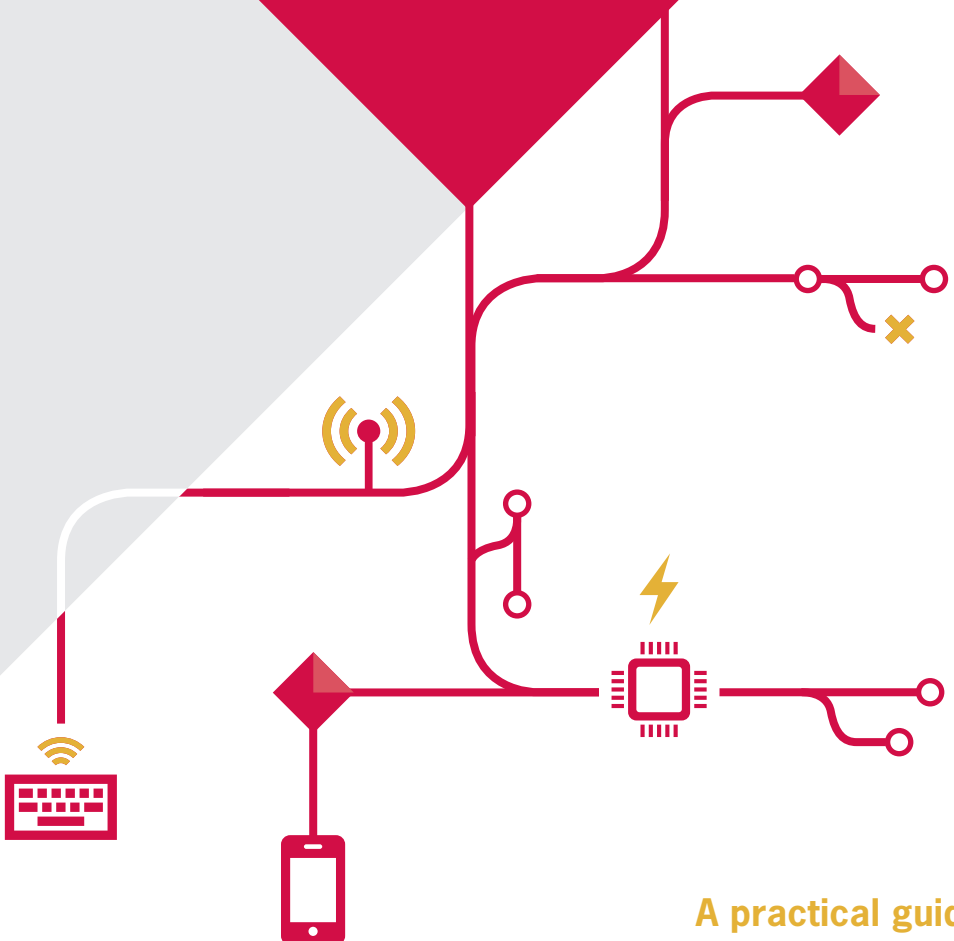




# The General Data Protection Regulation

25 May 2018  
Are you ready?



A practical guide to  
the changes ahead.

## WHAT'S CHANGED?

The European General Data Protection Regulation (GDPR) is landscape changing. Whilst most of today's data protection requirements remain, the introduction of the GDPR reflects the biggest change in European data protection laws in twenty years. The bar has been raised across the board, and there are a number of ground-breaking new concepts to tackle. As a result of its extra-territorial reach, many international businesses will, for the first time, be subject to European privacy laws.

Regulators will have bigger teeth: fines can be up to the greater of **€20 million or 4% of global turnover**.

The GDPR takes direct effect across Europe on **25 May 2018**.

We have been talking to clients about their preparations for the GDPR and we have been **listening closely** to their key concerns and the compliance challenges that they are anticipating.

Our clients have told us that they want *practical guidance* with a focus on the key areas of change. We are keenly aware that a literal interpretation of the GDPR could end up stifling business and slowing the innovation that our clients are known for. This document identifies the areas which are subject to the greatest change when compared to today's data protection regime, including guidance on what questions you should be asking, and what steps you should be taking towards GDPR compliance.

◆◆ Innovation is a Foot Anstey strong point. ◆◆

**Matthew Smith**  
Director of Legal, Screwfix

## HOW CAN WE HELP?

### ◆ Developing strategy and policy:

With accountability and data governance at its core, the GDPR means that data protection needs to be put 'front and centre' within every organisation. It goes without saying that our lawyers are technical experts in this area of law but, more than that, they have first-hand, in-house experience of dealing with the commercial realities of data protection compliance. We can help you at the earliest stages of planning your GDPR preparations by developing policy and strategy, engaging senior management and planning a programme with a timescale that works for your business.

### ◆ Data driven opportunities:

Increasingly, we find ourselves working on the development of cutting edge marketing and data management practices (including working on targeted and programmatic advertising, data management platforms and other advertising/marketing related technologies). Our experience of working deep within global commercial organisations means that we are able to offer more than just a 'plain vanilla' data protection advisory service. The GDPR shifts the goalposts. We can help you to work with, and extract value from, your data to make sure that you have the best possible business intelligence allowing you to truly know your customers in a way that minimizes your exposure to data protection compliance risks.

### ◆ Data mapping and audit:

We can help you to scope, design and conduct data mapping and audit exercises (data health check). We can be as hands on as you need, or we can take a more advisory role, helping you to produce template audit questionnaires and reports.

### ◆ Risk analysis and remediation strategy:

We will always take a commercial approach. We listen closely to clients to help identify, plan and prioritise any remediation work identified as part of the audit exercise, rather than simply suggesting that measures be implemented based on a black and white application of the legal framework.

### ◆ Design and implementation of detailed compliance processes:

We can help wherever changes are required to existing business practices, or if new processes or documents are needed. For example, the formal introduction of the data protection by design principle may require changes to IT procurement and HR processes, and the changes to the consent regime may require updates to marketing practices (such as online user journeys, privacy notices and opt-in mechanics).

### ◆ Training:

We can help you to establish, design and deliver training programmes for your staff, whether that is focused on strategic engagement at senior management level, or granular process driven training (such as in respect of marketing practice or breach notification processes) to specific teams within your business. Training is likely to be a crucial part of any robust compliance programme, since it actively demonstrates a culture of accountability and governance.

### ◆ Ongoing support:

Our lawyers are experienced at dealing with day to day data-related issues in a commercial environment. We can support you on an ongoing basis to manage your data protection compliance practices. Whether that takes the form of assistance with Data Protection Impact Assessments or specific data protection by design implementations, or ongoing/ad-hoc updates to policies or practices to reflect new business processes rolled out over time.

### ◆ Crisis management:

We are well placed and highly experienced in advising in the event of data security breaches, providing proactive advice on SARs and complaints by individuals, and sound strategic advice in the crucial area of reputation management and brand protection in the face of data protection breaches.

## GLOSSARY

**Controller:** The entity making decisions about the processing of personal data (e.g. a business will be a controller in respect of its customer data, marketing data and employee data).

**Processor:** The entity appointed by a controller to conduct certain specified processing activities in respect of certain data (e.g. a business may appoint different 'processors' to conduct payroll processing, marketing services or IT support/hosting services). Processors may be group companies or unrelated third parties.

**DPO:** Data Protection Officer

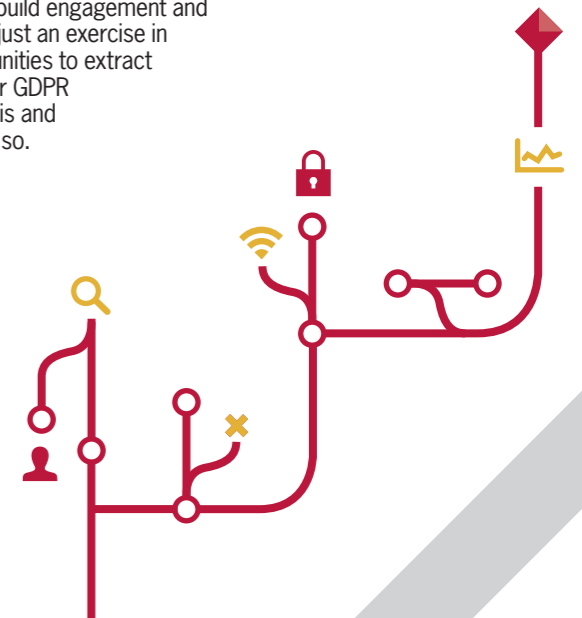
**DPDD:** Data Protection by Design and Default

**DPIA:** Data Protection Impact Assessment

**SAR:** Subject Access Request

## NEXT STEPS

- ◆ Consider accountability: put someone or a team in charge.
- ◆ Think carefully about your data subjects (customers, targets, employees etc). What outward-facing/public 'privacy profile' do you want to adopt? For example, are you aiming for industry best practice, or are you prepared to take a degree of commercial risk?
- ◆ Plan and carry out an audit and data mapping exercise. Start by thinking about what data you have and where it is.
- ◆ Assess risk and resource. Where are the biggest holes in your compliance picture, as revealed by your audit? Where are the biggest/easiest wins?
- ◆ Build data protection into your business culture: "bake it in".
- ◆ Raise awareness and give training. Make sure you tie your business processes into your implementation of the 'Accountability' principle.
- ◆ Lots of potential tripping points are largely a question of process: implement robust, tried and tested processes in advance (i.e. in relation to breach notifications).
- ◆ Look carefully at your existing privacy notices and consents. Consider the extent to which you will need to 'refresh' your consents to meet GDPR requirements.
- ◆ Lastly, find opportunities to help build engagement and make data protection more than just an exercise in compliance, e.g. look for opportunities to extract value from your data: getting your GDPR compliance right may facilitate this and will lower the risk profile of doing so.



# What's changing? Stay on top of data protection

## HIGHLIGHTS

## CONSIDERATIONS

## ACTIONS

ACCOUNTABILITY & AWARENESS



- ◆ "Accountability" is now a formal requirement.
- ◆ Be prepared to demonstrate that you are taking data protection compliance seriously.
- ◆ Mandatory DPO for some controllers and processors.



ACCOUNTABILITY & AWARENESS

DATA GOVERNANCE



- ◆ Onerous record-keeping obligations.
- ◆ You must practise (and demonstrate) DPDD.
- ◆ DPIAs will be compulsory in certain circumstances related to the level of risk presented by your use of data.
- ◆ There is now a legal requirement to have a data protection policy.



DATA GOVERNANCE

OUTSOURCING & PROCESSORS



- ◆ Contracts with third party processors will need to contain additional specified language.
- ◆ Obligations must flow down to any sub-processors engaged by your suppliers.
- ◆ Processors will be on the hook for certain aspects of GDPR compliance in their own right (e.g. record keeping, security, breach reporting to the controller and international transfer restrictions).



OUTSOURCING & PROCESSORS

INFORMATION NOTICES & CONSENT



- ◆ New requirement to ensure "transparency" of data processing in addition to existing requirements for "fairness" and "lawfulness".
- ◆ There is now a longer list of information that needs to be provided in your privacy notices to individuals, but conversely there is a focus on clear and concise information notices that are easily accessible and easy to understand.
- ◆ Consent requirements are significantly more robust. Consent will be harder to obtain and harder to rely on.
- ◆ The use of 'bundled' consents will no longer be valid: consents must be granular and distinguishable from other terms.
- ◆ Consent will now require affirmative action which is likely to mean an end to pre-ticked opt-ins and inferring consent from silence and/or inaction.
- ◆ Historically obtained consents will need to be brought into line with the GDPR's new requirements.
- ◆ Be aware that the GDPR contains specific provisions in relation to children's data. Notices and consent language may need to be drafted with children in mind and you may need to consider parental consent mechanics.



INFORMATION NOTICES & CONSENT

INDIVIDUALS' RIGHTS



- ◆ Rights have been extended (for example there are new rights to erasure, portability and restriction of processing) and rights are easier to exercise.
- ◆ Timeframes to comply with the exercise of rights are shorter (one calendar month).
- ◆ Data provided in response to a SAR must be provided free of charge. Removal of the ability to charge a fee has a significant impact on timing and process since the clock will start ticking straight away (whereas, pre-GDPR, the clock is stopped until the fee is paid).



INDIVIDUALS' RIGHTS

BREACH NOTIFICATION



- ◆ The breach notification regime has been completely overhauled. There are now formal notification obligations.
- ◆ Controllers must notify the relevant supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of a breach.
- ◆ Processors must notify controllers of a breach without undue delay after becoming aware of it.
- ◆ New obligations to notify affected data subjects in certain circumstances.
- ◆ New obligation to maintain an internal breach register.



BREACH NOTIFICATION

- ◆ Who is in charge of data protection matters in our organisation? Do we have buy-in at Board level?
- ◆ What might need to be delegated to different teams (e.g. HR, IT, compliance/legal) to make sure that awareness flows down and that accountability flows up?
- ◆ Will we need a DPO? If not, do we want a DPO?

- ◆ What personal data does my organisation process? For what purposes? How is it collected? Where is it stored, accessed and used? Who else processes it and what for? How long is it kept for and why?
- ◆ Do we have (or could we create) records of our processing activities?
- ◆ Could we pseudonymise or anonymise any of our personal data?
- ◆ Is privacy built into our organisation's business processes? If so, how is this documented?
- ◆ How will we evaluate whether or not a DPIA is required in each case? What process will we follow and who will 'sign-off'?
- ◆ Where are our processes documented/how are these implemented?

- ◆ Who else processes the personal data that my organisation controls?
- ◆ What contract terms do we have in place with our third party processors, and what have we done (or can we do) to check whether they have appropriate data protection compliance practices (e.g. have we audited their information security?)
- ◆ Are any sub-processors involved further down the chain?
- ◆ Do we process personal data on behalf of anyone else (i.e. do we need to be aware of new obligations in our role as a data processor?)

- ◆ Are our privacy notices compliant with the new GDPR requirements? Can we provide all of the additional information (e.g. do we have documented retention periods, can we describe our reliance on the 'legitimate interests' basis for processing?)
- ◆ Where in our business do we rely on consent (e.g. marketing consents, international transfer)?
- ◆ How robust are our consents when viewed alongside the new requirements?
- ◆ Do we rely on bundled/pre-ticked boxes or consent 'hidden' in our terms and conditions?
- ◆ What level of risk are we happy to accept when looking at our historic consents (when compared to the effort and consumer experience associated with an exercise to 'refresh' our consents)?
- ◆ Are any third parties involved in data collection? If so, are we confident that the opt-ins/consents they obtain are sufficient?
- ◆ Do we process children's data? If so, do we rely on consent as a basis for processing this data?

- ◆ Do we have processes in place to deal with individuals exercising their rights?
- ◆ Would our staff recognise an SAR or other exercise of rights? Would they know what to do?
- ◆ Do we retain too much personal data or for too long (i.e. are we making our job too difficult)?
- ◆ Is the right to erasure (the 'right to be forgotten') or the right to data portability likely to affect our business? If so, how would we deal with these in practice?

- ◆ Do we have measures in place to minimise the risk of breaches occurring (both technical measures, and operational/organisational measures)?
- ◆ Would our staff recognise a breach? Would they know what to do?
- ◆ Who would be responsible for co-ordinating the internal response to a breach and the accompanying investigation and mitigation activities?
- ◆ Who would be responsible for external communications (with regulators and data subjects where necessary)?

- ◆ Determine whether you need a DPO (very broadly speaking: public bodies, processors of particularly sensitive data, 'big data' companies). Consider carefully whether you should voluntarily appoint a DPO: they will need to be able to operate with independence and will have employment protections relating to the role.
- ◆ Put someone in charge and put together a team. Start raising awareness among key internal stakeholders.
- ◆ Start working on a 'paper trail' to assist with the GDPR's record keeping obligations.

- ◆ Start 'mapping' your organisation's data and investigate key aspects of your data protection practices against GDPR requirements.
- ◆ Identify where and how data protection can be 'baked-in' to documented processes and practices.
- ◆ You will need to be able to demonstrate 'data protection by design and default', you will need to conduct (and record) DPIAs wherever processing is 'high risk'.

- ◆ Audit the use of third party processors in relation to personal data.
- ◆ Review contract terms and start discussions with processors in respect of the new GDPR obligations.
- ◆ Consider whether you have appropriate liability protections to deal with the shift in the default liability position under the GDPR.
- ◆ Review practices relating to third party processors in light of DPDD, DPIAs and record keeping obligations.
- ◆ If your organisation processes personal data on behalf of other businesses, you will now have your own legal obligations in respect of that data, and not just those in your contract with the data controller.

- ◆ Audit all of your privacy/information notices against the new list of requirements set out in the GDPR including in respect of content, accessibility, ease of use and format.
- ◆ Consider ways to make your information notices more 'digestible' (giving particular thought to the profile of your customer base/audience) e.g. layered notices, graphics, videos or summaries.
- ◆ Conduct an audit to identify data processing activities that rely on consent as a legal justification for the processing.
- ◆ Review consents with a view to determining whether, in fact, there are other legal bases for processing that may eliminate the need to rely on consent (e.g. can you rely on the performance of a contract?).
- ◆ Where necessary, update consent language and mechanics (and related business processes) in order to meet the new requirements.
- ◆ Consider whether any third parties are involved in the provision of information notices or the collection of consents. Ensure that contract terms are appropriate and that they address notice and consent.
- ◆ Pay particular attention to any notices and consent language/mechanics relevant to the use of children's data. Consider how you might obtain parental consent if necessary.

- ◆ Review existing processes in your business used to deal with SARs and other data protection related rights.
- ◆ Consider issuing training or guidance on SARs and other rights to relevant employees (e.g. HR, IT, consumer-facing staff) to raise awareness, including in relation to timeframes and specific obligations.

- ◆ Review your security measures and other operational and organisational measures to minimise your breach risk.
- ◆ Review existing breach-related processes. The timeframes are extremely short. You will need to document decisions taken relating to breaches (e.g. whether or not to notify regulators and individuals). Clarify who should be involved and who ultimately needs to sign off on relevant decisions.
- ◆ Implement technical measures (such as encryption) to ensure that breached data is not readable, since this is likely to eliminate the need to notify regulators.
- ◆ Review contracts with third party processors to ensure that the terms include robust breach notification (and subsequent cooperation) obligations.

## CONTACT US



**Martin Cuell**  
**Partner**  
martin.cuell@footanstey.com  
07989 968754



**Alexandra Leonidou**  
**Senior Associate**  
alexandra.leonidou@footanstey.com  
07980 776152



**Tony Jaffa**  
**Partner**  
tony.jaffa@footanstey.com  
07770 223993



**Jo Vale**  
**Solicitor**  
jo.vale@footanstey.com  
07896 428377