It's Time to Get Ready for GDPR

(General Data Protection Regulation)

Briefing on Europe's new data protection law.

Cordery Legal.Compliance

Company85 accomplish more™

iomart

Executive Summary of GDPR Changes

Introduction

The data protection and security landscape is all set for change with the advent of the new EU General Data Protection Regulation ("**GDPR**") in May 2018. Yes there will be regulatory burdens but make the new system work for you.

- The new rules are part revolution/part evolution - the new system builds on the current familiar one;
- Don't panic, plan instead - the full impact will come in May 2018 but preparation now will pay off then.

Reach

The new rules will apply to all those in the EU who control data and/or undertake data processing.

- All sectors are affected - the more robust your privacy compliance the better your market advantage;
- Non-EU businesses doing business in the EU are also affected.

New rights

New rights are being introduced and existing ones tweaked, including:

- A new Right To Data Portability;
- An extended Right To Be Forgotten
- An enhanced Subject Access Right - to be free and a shorter reply timescale.

Data Protection Impact Assessments ("DPIAs")

DPIAs will have to be undertaken for certain data processing operations.

- DPIAs put the compliance assessment burden on those handling personal data - but, used as a wider tool they help you get a better handle on your data processes and reduce risk, thereby building privacy as an integral compliance element in your business, and, they can help with security auditing.

Security breach reporting

One of the most important changes is that there will be mandatory data/security breach reporting.

- Breaches must be reported to a regulator within 72 hours and those affected by the breach must also be informed - to do this you must have clear, practical, effective and immediate procedures, and, get your vendors on board - it is so business critical you can't afford to get it wrong.

Greater penalties

Increased enforcement will come about with the new regime, backed up by greater sanctions.

- For certain infringements a maximum fine of Euro 20 million or 4% of the global annual turnover of a business (whichever is the greater) can be imposed, with likely higher reputational damage resulting - this is the big stick for data protection compliance, but, getting it right will avoid major headaches.

What you need to do now?

Start preparing now and complete the short action plan at the end of this document.

Now is the time to get ready for widespread changes in data protection and data security law in Europe.

Data protection and data security have been hot topics over the last 2 or 3 years. Barely a day goes by without a news story about a data breach, an infringement of privacy or an inappropriate use of personal data. It's been difficult for some businesses to adapt and hard-earned reputations have been lost in days – and the legal framework is about to get tougher still with the new European data protection law, the General Data Protection Regulation ("**GDPR**") which will come into force in May 2018.

It introduces mandatory breach notification for the first time and greatly increases the financial penalties for non-compliance. It's something that needs board-level attention and guidance – that's why we've published this paper.

The GDPR is a major change in European Union ("**EU**") data protection rules aimed at bringing privacy laws into line with the technological leaps of the digital age. The European Commission has promised that the new rules will bring a uniform regulatory regime, fewer administrative burdens, reduced costs, improved and increased rights and make privacy by design the norm.

Whilst only time will tell if they live up to this, the high value placed on data today is undisputed and so those businesses with a robust approach to privacy compliance will have a distinct market advantage.

This paper – written by Cordery specifically for customers and contacts of Company85 - looks at the key changes GDPR will bring and suggests practical steps to help you comply. It covers most of the main issues with the new law including:

- What are the new rules on security breach reporting? (Pg 4)
- How have penalties increased? (Pg 5)
- Who does the law affect? (Pg 6)
- What are the new rights GDPR introduces? (Pg 7)
- What is the DPIA process? (Pg 8)
- How will the auditing regime work? (Pg 9)
- What do you need to do now? (Pg 10)

The UK data regulator the Information Commissioner's Office ("**ICO**") said in March 2016

"You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have."

This paper will help you do that.

The GDPR regime will bring significant changes – but there's no need to panic. With proper planning there is still time to be ready for the GDPR and to deal with the worst effects of a data protection lapse. The ICO has stressed the need for proper planning saying "It is essential to start planning your approach to GDPR compliance as early as you can and to gain 'buy in' from key people in your organisation. You may need, for example, to put new procedures in place to deal with the GDPR's new transparency and individuals' rights provisions." In this paper we look at some of the key aspects of the GDPR and some of the challenges it brings, but we also look at some solutions. Putting proper plans, policies and procedures in place now will help you reduce the risk and ensure that you are ready for the new law when it comes in.

What are the new rules on security breach reporting?

Ensuring that data is secure is one of the cornerstones of the new rules. To do this the GDPR has introduced mandatory reporting of data breaches to the regulator and communication of breaches to those affected.

What exactly is a personal data breach? Under the GDPR it is defined 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." Breaches will have to be reported under a framework set out in the new rules including what action has been done to mitigate them.

The report must be made to the relevant data protection regulator (or regulators) without delay and, "where feasible", not later than 72 hours after a data controller has become aware of the breach.

A reasoned justification must be provided where reporting is not made within the 72-hour period.

There is however an important caveat to the breach reporting obligation as it will not apply where "the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals."

There is a second reporting obligation too. Under what some are calling "the right to know when your data has been hacked", the breach must be communicated to those affected by it, subject to certain conditions and "without undue delay" (but no time-limit has yet been set). There are some limited exceptions to this obligatory communication requirement, for example where the data affected by the breach has been encrypted, although it is unclear what the encryption standards will be at this point in time. Since some of the fine detail (including the time you have to make the communication) may be down to local regulators you'll need to take expert legal advice if you have a breach. You'd be wise to take advice even if you think you can rely on any exemption.

Clear, practical, effective and immediate procedures are going to be needed to address security breaches. They are high risk – not only because of likely regulatory enforcement but also because of what else is at stake, including reputation. This is a top priority.

People panic after a data breach so policies need to help them through their response. This also means special training must be undertaken for those who will be directly involved which should also cover how and what to communicate to customers - the CEO should be the first one to be trained.

The procedures should also be regularly tested and evaluated and rehearsals carried out. The recent past has shown us that data breaches can get ugly, especially if the response isn't adequate and the tone at the top is wrong. Data breaches do happen to most companies and it's often a bet-the-company situation when they do – businesses need to invest in process accordingly.

In addition businesses still need to do all they can to stop breaches happening. Agreements with vendors will be key.

You will need to ensure your vendors care about data security but your agreements also need to ensure their cooperation in reporting to regulators when bad things happen.

Organisations will also need to run their own due diligence to identify high-risk vendors.

It is also worth adding here that, in addition to the GDPR, there will also be new (separate) EU cyber security rules. A new EU Directive requiring EU Member States to improve their national cyber security capabilities and co-operation between them has been agreed upon at the EU political level and awaits finalisation. These rules will require security measures to be in place and incidents reported to national authorities by operators of critical infrastructure in financial services, transport, energy, water and health and enablers of information services such as internet payment, cloud computing and search engines. The full details of the agreed text still need to be made available but it is understood that the main blocks of the new rules are that:

(i) the EU Member States must adopt a Network and Information Security ("NIS") strategy and designate a national NIS authority to be able to prevent, handle and respond to NIS risks and incidents (to include Computer Response Teams);

(ii) an EU co-operation mechanism must be set up between EU Member States and the European Commission to share early warnings on risks and incidents;

(iii) the types of organisations mentioned above will have to assess the security risks they face and adopt measures accordingly, and report to their relevant national regulators serious security incidents on their core services.

GDPR became law on the 25th of May 2016 and will be in force in two years i.e. May 2018.

There is expected to be quite a few variations between the Member States in their implementation of the rules given that this is a Directive and not a Regulation which allows for differences on a country-by-country level. If organisations fall under these new rules they will therefore also have to factor in this extra breach reporting requirement.

How have the penalties increased?

One of the very significant changes of the GDPR is that data protection regulators will have the power to impose high fines for infringing the new rules. Three different bands of fines will be applied in relation to three different sets of categories of infringements.

The highest level of penalty is either a maximum of Euro 20 million or 4% of the global annual turnover of a business, whichever is the greater.

This will apply to the category of infringements concerning non-compliance with one of the listed corrective orders of a regulator.

Parallels have also been drawn here with competition law, for example with regard to using a methodology of aggravating and mitigating factors in terms of how a penalty sum will be finely tuned.

Given the potentially higher fines for infringements, which would also cause significant reputational damage, the data protection compliance drive for businesses will now be even more of an imperative.

Who does the law affect?

The new rules will apply to all organisations in the EU who control data and/or undertake data-processing. All sectors are covered, including IT. A data controller is any person, company etc. who determines how and for what purposes personal data are processed. Data-processing means obtaining, recording, holding, or carrying out any operation on personal data. Personal data is data relating to a living individual who can be identified from that data.

Most operations in relation to personal data will constitute processing and because the definition of processing is very wide, as the UK regulator the ICO puts it, "it is difficult to think of anything an organisation might do with data that will not be processing."

In addition, data controllers and processors will also have considerably more responsibilities and obligations under the new rules. Data controllers will have to implement technical and organisational measures to ensure (and be able to demonstrate) that the processing of personal data is performed in compliance with the new rules, including the implementation of data protection policies.

Data processors will now have to maintain records of all their processing activities, to be disclosed to demonstrate compliance when required.

User-friendly manageable practical processes can all be put in place to guarantee that these new requirements are observed by controllers and processors. Whilst data management will become more encompassing it will at the same time benefit organisations as they will have a more secure grip on where their data is and where it goes.

The fact that the new rules will apply to all organisations actually located in an EU Member State is not an innovation (the current rules also apply to everyone in the EU). What is more radical is that they will also apply to businesses located completely outside the EU. This will be the case where either:

- a business processes the personal data of EU residents and offers them goods or services, irrespective of whether payment is required; or
- where the processing by a business relates to the monitoring of the behaviour of EU residents in so far as their behaviour takes place within the EU.

The aim is to have a level playing-field and thereby help businesses in the EU. But how can we tell if the long-arm of the GDPR applies? The new rules provide some guidance. The mere accessibility of a business' website in the EU or of an email address and of other contact details or the use of a language generally used in the country outside the EU where the business is established will not be enough to bring a business under the new rules. But, factors such as:

- the use of a language generally used in one or more EU Member State with the possibility of ordering goods and services in that other language;
- the ability to pay in a currency used in one or more EU Member States
- mentioning customers or users who are in the EU

could be relevant in determining that a business offers goods or services to EU residents. If it does then that business would likely be caught by the GDPR.

If it comes within the GDPR regime a business located outside the EU will also have to designate (in writing) a representative in the EU. That representative may be subject to enforcement action for non-compliance.

What are the new rights GDPR introduces?

There has been a steady increase in reliance on data protection rights over the years. We've seen more and bigger legal cases such as the notorious Schrems case concerning transfers of data from the EU to the US. Under the GDPR the use of data protection rights can be expected to become more aggressive and will generate more litigation.

Generally-speaking an overarching aim of the GDPR is for individuals to have easier access to data about them - individuals will have more information on how their data is processed, which should be made available in a clear and understandable way. You'll probably need to update privacy policies as a result. But the GDPR also goes further in that new rights are being introduced that allow individuals more control over data held about them. Two of these rights and a new aspect to an existing commonly used right are explained below.

The GDPR introduces the so-called "Right To Be Forgotten". This means that an individual has the right to have personal data erased by a data controller "without undue delay", based on certain grounds, for example, where "the data is no longer necessary in relation to the purposes for which they were collected or otherwise processed", or, where an individual has withdrawn consent on which the processing is based. This is a much wider right than the one that was set out in the European Court's 2014 widely-reported ruling in the Google case, notably because that ruling strictly applied only to search engines. But it must also be stressed that this is not an absolute right: for example, further retention of the data will be lawful in some limited cases such as where it is necessary to comply with a legal obligation or to exercise the right to freedom of expression and information.

This right has advantages and disadvantages. On the positive side, it will help people remove an emotional burden where their privacy has been invaded and exposed and emotionally hurt them, such as where their children have been named or photographed in relation to traumatic circumstances. On the negative side probably the greatest risk is that some people will use this right (and following the Google case some have already been relying on it) to hide their unsavoury past and others may then come to rely on a modified and ultimately misleading version of a person's life and expose themselves to a risk or even danger when making decisions concerning that person.

The practical approach to dealing with the "Right To Be Forgotten" is to set up an internal across-the-board process in order to meet these requests, which includes the technical, logistical and costs aspects.

For example, this could consist of a policy document which sets out internal criteria to address the key issues - this could include a checklist on how to decide where "the data is no longer necessary in relation to the purposes for which they were collected or otherwise processed".

The GDPR also introduces the "Right To Portability". Essentially this means that people will be able to transmit personal data from one data controller to another without hindrance. An individual will be able to receive a copy of the personal data which they have provided to a data controller in a "structured, commonly used, machine-readable and interoperable format and transmit it to another controller". Where feasible, individuals should have the right to have their data directly transmitted from one controller to another. The right applies where the person concerned has provided the data based on contractual consent or where the data is necessary for the performance of a contract, and the processing is carried out by automated means. The right does not apply in certain circumstances, for example, where controllers are processing data in the public interest.

The practical approach to dealing with the "Right To Portability" is to ensure that technical systems can efficiently retrieve and transfer individuals' data to others, and that security systems are robust enough to prevent disclosure of third party data to unauthorised recipients - ensuring the latter will present challenges but they are not insurmountable. The GDPR also encourages (but does not oblige) controllers to develop interoperable formats to support data portability - businesses should therefore consider developing workflows to retrieve and share data in such formats.

The existing so-called "Subject Access Request" ("**SAR**") is a process under which someone can exercise their right to gain access to data held on them. There has been a significant rise in the number of SARs being made in recent years. The fee you can charge and the time you have to comply with a SAR varies across Europe but in the UK currently you can charge up to £10 and you have to reply to a request 'promptly' and within a maximum permitted time of 40 days.

Under the new GDPR a request must be answered within one month of receipt of the request, but this may be extended for a maximum of two further months when necessary depending on the complexity of the request and the number of requests. The GDPR also abolishes the ability a business has to ask for a fee.

When SARs become free we are likely to see even more requests being made. Given the prevalence of email and cloud applications in particular SARs are also now more costly and complex to deal with.

Therefore, a key part of any organisation's future data protection strategy under the GDPR will be to put in place proper processes that factor in an efficient use of resources to deal with SARs, especially within a short timeframe.

Do you know how to respond to requests? Do you know when exemptions apply to your business, so you don't have to waste valuable time and money on requests that you need not comply with? Can you locate, categorise, review and redact all emails and other personal data in less than a month? If you can't you will need to design processes now to help you comply. Proper training and task allocation to the right people will also help.

What is the DPIA process?

Privacy by design and/or default will not be just a 'nice to have' under the GDPR – it's a core part of the new law, and, there's a mandatory process businesses will need to adopt in certain circumstances but which is a useful tool to adopt across-the-board. This process is called a "Data Protection Impact Assessment" ("**DPIA**").

Under the GDPR there will no longer be a requirement for a data controller to routinely register with a data protection regulator, and consequently the payment of a fee to register will also disappear.

The DPIA system effectively replaces the old registration regime – and it puts the burden for assessing the compliance needs firmly on the shoulders of any business handling personal data.

Our experience though is that DPIAs should not be feared. We know from the projects we have worked on that DPIAs can bring real benefits to an organisation - their use is recommended beyond the circumstances when they are mandatory. Properly used they help businesses look more closely at the processes and procedures behind a new offering and they reduce risk.

When you introduce new products or services it is a good idea to do a DPIA as this will help you build in data protection safeguards into your products and services from the beginning including measures such as data security by design, minimising the processing of personal data, and, anonymising personal data, to be introduced as soon as possible and to enable an individual to monitor the processing of their data.

Where processing operations (especially on a large scale) are likely to result in a high risk for the rights and freedoms of individuals, in particular using new technologies, a DPIA of the planned processing operations on the protection of personal data must be carried out, prior to the processing starting. This must be done to take into account the nature, scope, context and purposes of the processing. Regulators are still involved however. A regulator can ask to see the DPIA you have done and a data protection regulator must be consulted prior to the processing of personal data where the DPIA indicates that the processing would result in a high risk in the absence of measures taken by a data controller to mitigate the risk.

There is no 'one size fits all' DPIA process. Effectively the DPIA process involves a risk and cost-benefit analysis and a list of measures the business could take to mitigate risks.

Sometimes businesses won't go through the full DPIA process as an initial analysis will make it clear that the risks are too great or the benefits not enough to make it worthwhile. DPIAs are one of the measures which can add benefit to a business now. We are already seeing our clients invest in robust DPIA processes and staff training. Some of our clients have already identified security vulnerabilities in what they do using a DPIA process. Starting with DPIAs now means the two year lead time can also be used to make sure that a proper assessment process is embedded into the business.

It also means that any future products or services the business is designing now should be compliant with the new GDPR regime.

How will the auditing regime work?

Under the GDPR regulators have the power to "carry out investigations in the form of data protection audits" and "to obtain access to any premises of the controller and the processor, including to any data processing equipment and means". Regulators already have similar powers in the field of healthcare and financial services, which they have exercised, but what is new is that now there will be across-the-board rules, which will apply equally to the private and public sectors.

Organisations will therefore need to be prepared to be subject to audit and to put in place a proper auditing methodology.

Also, because the ICO will be able to carry out unannounced dawn raids organisations will need to put in place procedures and train staff to deal with this possibility. This too can be dealt with in straightforward practical terms and business can learn lessons here from their experience with competition law where similar staff skills training could be applied.

What you need to do now?

GDPR is a vast piece of work with over 200 pages of legislation. This note gives just a highlight of the main issues and what you will have to do will depend on what your business does with data. That being said every business needs to plan now for the GDPR. The preparatory work for compliance with the new rules must start now – many companies are already doing this. The following is the action plan we recommend you start with:

- Brief the board - get it across to them that the new rules are a top compliance priority;
- Do a gap analysis - determine where your vulnerabilities lie and think about plugging gaps;
- Audit your information assets - start now with a data protection impact assessment;
- Give sharper focus on how you engage with vendors - you will need proper due diligence and comprehensive legal agreements;
- Design the DPIA process you will use;
- Start updating procedures and policies (especially in case of data breaches) and prepare new detailed documentation - have records ready to be produced for regulatory inspection; and,
- Train staff on all of the above. One-size-fits all training won't work but a clear program starting now will help prepare for GDPR and reduce data protection and security risks now too.

There will be lots of scaremongering around GDPR. We are also already seeing pressure groups gear up for a fight, looking forward to the greater power they will have. Proper planning can avoid a last-minute panic. The time to start on your plan is now.

How Company85 and iomart can help IT prepare for the changes

GDPR is just one challenge in an evolving landscape, but its consequences will be felt across all departments, including information security. Company85 and iomart commissioned this guide to help IT teams understand the implications of the legislation and encourage them to start the planning and strategic work now.

Company85 and iomart have a suite of services to help you kick start your work around GDPR and to ensure that your systems and processes are more than merely compliant but also robust enough to support the future of your business

GDPR QuickStart

GDPR QuickStart rapidly frames your GDPR needs, either by outlining and prioritising the steps towards compliance, or by calling upon industry expertise to validate your existing approach. Our GDPR experts will run workshops and interviews with key stakeholders and SMEs within your organisation to assess the impact of the GDPR. The workshops will look at the requirements of the regulation and the ability of existing people, process and tools to meet those requirements. Where gaps are identified, potential solutions to address or mitigate them will be proposed, including an infographic designed to be shared with your board.

Contact iomart to find out more.

Company85
accomplish more™

Company85 is an independent IT consulting firm specialising in enterprise-class information protection, transformation and service management.

Headquartered in London, we provide advisory, implementation and managed services to FTSE100 companies and public sector organisations across the UK, Europe, Africa, the Middle East and the US.

Our clients include AstraZeneca; BBC; Betfair; Deutsche Bank; EE; Financial Times; Greater Manchester Police; J.P.Morgan; JLT; Lloyds Banking Group; Lloyds of London; LOCOG; NHS; Pfizer; RBS; Roche; Royal Mail; and Vodafone.

iomart

Iomart Group Plc is the most accredited provider of managed cloud services in the UK. From strategy to delivery, our 300+ consultants and solutions architects provide the cloud expertise to help organisations maximise the flexibility, cost effectiveness and security of the cloud.

Headquartered in Glasgow, Scotland and listed on the London Stock Exchange, we own and operate a network of UK data centres and provide our cloud expertise to public sector organisations, enterprises and SMBs.

Our clients include: Go Ahead, Pernod Ricard, UK Parliament, Calastone, Liverpool FC and British Red Cross.

Lister Pavillion, Kelvin Campus, West of Scotland Science Park, Glasgow, G20 0SP
0800 040 7228 • info@iomart.com • www.iomart.com