POINTSHARP

GDPR compliant email

A practical guide to getting on top of the latest changes to requirements with some suggestions of quick technological wins for your enterprise

pointsharp.com

Table of contents:

GDPR Compliance, a practical guide to getting on top of the latest changes to requirements with some suggestions of quick technological wins for your enterprise.

Management summary and conclusions

The European Union has for a long time seen data privacy as an important issue and has worked hard to create a unified legislation to protect the interests of all citizens of the EU whose data may be held for one reason or another inside or outside the EU. This of course is not entirely new legislation - the original working drafts dating back to 1995 - however in the latest form it does include some significant new provisions with far reaching impact.

Several major and minor new terms will require careful consideration by all organisations, large and small, and we conclude several things having talked to representatives of the EU, to our customers and to customers of other technology vendors, in the USA, EU and APAC. These are that:

- Most organisations have implemented some of the protections they need, but few have covered all bases. There is work to be done.
- Non-EU based companies have much more to do and may be more vulnerable under scrutiny. Time to catch up.
- Technology is key to solving the issues, but soft requirements (people and behaviour) cannot be ignored. Few organisations have allocated sufficient money or time to handle these new demands.
- Use established technology such as email, but solve known issues of large file handling and security first. Why? You can implement this fast and place a known solution in front of all users for a far more predictable win.
- This may be a great time to get rid of some legacy technology and replace it with more modern, cheaper, more focussed solutions that do what you need and don't cost a fortune for what you do not need.
- Severe penalties will galvanise actions, but this is leading to a feeding frenzy by vendors making unjustifiable claims about their "unique" approach. The mirrors are everywhere and the smoke is thick.en werden.

Introduction

The recently ratified General Data Protection Regulation GDPR entered law on May 25th 2018. The objectives of this latest draft are summarised as:

There are pre-existing strong local laws in member states of course such as the German BDSG, (widely seen as a template for GDPR) which have been brought together with far reaching implications for all enterprises since these new laws extend far beyond the borders of Europe and have far greater financial penalties attached to a breach. Why, because compliance with the rules is determined by the domicile of the person whose data is held, not the location of the organisation that holds the data, so an enterprise based in the US with customers in the EU will need to gain an understanding of the demands of these laws and take appropriate actions to avoid severe penalties.

The emphasis of GDPR is to protect data rather than just keep it private and whilst that may sound a narrow differentiation this short guide is to identify the key changes and to show how protection may be possible by enhancement to existing technologies which in the past have been seen as failing basic rules of privacy and of protection.

For most enterprises, the latest changes to the GDRP legislation should be viewed as a long overdue prompt to consolidate and improve both technology led initiatives and organisational behaviour in the face of growing external scrutiny. That scrutiny of course is reflective of an ever-increasing general level of threat to data about individuals. This paper will deal with technical issues, but will also point to how these may affect your organisation and your staff.

Finally, the real driver to action for all enterprises is that now the penalties are so severe that inaction is not an option. These new laws have teeth.

‘The proposed new EU data protection regime extends the scope of the EU data protection law to all foreign companies processing data of EU residents. It provides for a harmonization of the data protection regulations throughout the EU, thereby making it easier for non-European companies to comply with these regulations; however, this comes at the cost of a strict data protection compliance regime with severe penalties of up to 4% of worldwide turnover. The Parliament‘s version contains increased fines up to 5%. After three way negotiations between the European Parliament, the European Commission and the Council of Ministers, there is general consensus on the wording of the GDPR and also the financial penalties for non-compliance. Controversial matters include Data Portability, One stop shop for the rules and the mandatory appointment of a data protection officer.’

What are the aims of the GDPR and what has changed?

The objective of the GDPR is to protect the data privacy of all EU citizens in an increasingly data orientated world, now vastly different from the aims in which the 1995 directive was established. Whilst the main principles of data privacy still hold true to the original directive, important changes have been proposed in the regulations. Some key points of the new GDPR as well as discussion of the impacts it may have on organisations can be found below.

Increased geographic scope (extra-territorial applicability)

One of the biggest changes in the regulatory landscape of data privacy comes with the extension of the jurisdiction of the GDPR, since it applies to all companies processing the personal data of data subjects residing inside the Union, regardless of the company's geographic location. Previously, territorial application of the legislation was ambiguous and referred to data processing in the context of an 'establishment' and this topic has come up in a number of high profile court cases. The new GDPR makes its applicability crystal clear. It applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of all personal data of data subjects in the EU by either a controller or processor not established in the EU, where the activities relate to offering goods or services to EU citizens (irrespective of whether payment is required) and to the monitoring of behavior that takes place within the EU. Non-EU businesses processing this data about EU citizens will also have to appoint a representative in the EU.

Penalties

Strong new penalties can be applied where organisations in breach of GDPR can be fined up to 4% of their annual global turnover or €20 million (whichever is greater). This is the maximum fine that could be imposed although only for the most serious breaches, for example not having evidence of sufficient customer consent to process data or violation of the core of Privacy by Design concepts. A tiered approach to fines is proposed, meaning a company could be fined 2% for not having their records in good order (article 28), failing to notify the supervising authority and data subject about a breach or failing to conduct an impact assessment. It is an important twist to remember that these rules apply to both controllers and processors which means that 'cloud vendors and suppliers' will not be shielded from GDPR enforcement.

Data Subject Rights

So, all of these new rules are designed to protect EU citizens, or those who are the subject of the data held. So what is new here?

Breach Notification

Breach notification will now become mandatory in all member states where a data breach has the possibility to "result in a risk for the rights and freedoms of individuals". This notification must be done within 72 hours of the data controller first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach. Whilst this is slightly more vague, the 72 hour rule is likely to be applied. Far better not to have a breach, so organization should make sure stored data is tightly protected and that rules are complied with.

Right to Access

Included in the broader rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller must provide a copy of the personal data, free of charge, in an electronic format. This change is a significant shift to the data transparency and empowerment of data subjects. If requested you will need a secure transport service that works in a fully ad hoc manner to fulfil this request. Logically this leads to the 'Right to rectification' where the data subject can provide the correct information and it must be corrected 'without undue delay'. You can just Imagine the challenge for a credit rating agency or insurance company!

Right to be Forgotten

This is also referred to as 'Data Erasure', specifically the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further sharing or use of that data and potentially ensure third parties halt all processing of the data.

The conditions for erasure, are outlined in article 17 and include that the data is no longer relevant to original purposes for processing, or that a data subject withdraws consent or places restrictions on processing. It should also be noted that this right requires controllers to compare the subjects' rights to the 'public interest' in the availability of the data" when considering such requests. This could be challenging. Think of all the ways you use data, and how copies may be left in data graveyards. Data should be purged after use to avoid this.

Data Portability

GDPR introduces rules for data portability or the right for a data subject to receive the personal data concerning them, which they have previously provided 'in a, commonly used and machine readable format' and to transmit that data to another controller on request. Again, an ad hoc transfer requirement, where encryption of data in transit is of the essence.

Consent

The conditions for consent have been made more stringent, and companies will no longer be able to use long confusing terms and conditions full of small print since the request for consent must be given in an intelligible and easily understood form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other questions and be provided in a legible format, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Privacy by Design

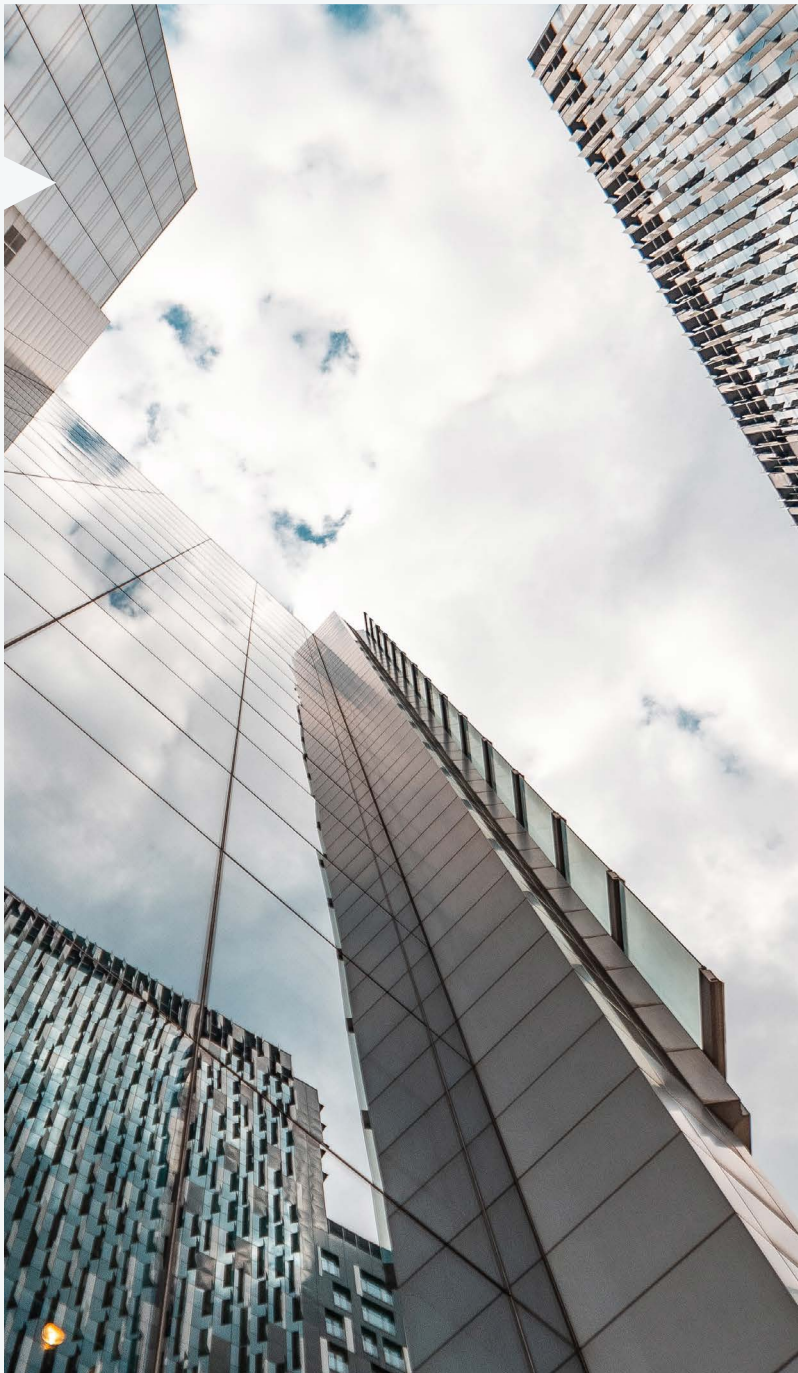
Privacy by design has existed as a concept for years now, but it is only now becoming part of a legal requirement with the GDPR. At its heart, privacy by design calls for the inclusion of data protection from the outset of the design of systems, rather than as an addition. That is not to say that good systems such as email cannot be improved, but it does demand the issues are thought through and systems are in place that remain compliant.

To be more specific; 'The controller shall implement appropriate technical and organizational measures in an effective way in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 25 calls for controllers to hold and process only the data that is absolutely necessary to fulfill its duties otherwise called data minimization, in addition limiting the access to personal data to only those needing to act out the processing tasks.

Data Protection Officers (DPO) required

Today controllers are required to notify their data processing activities with local Data Protection Authorities (DPAs), which, for multinational organisations, can be a bureaucratic mine-field since most member states have different notification requirements. Under the new GDPR it will not be necessary to submit notifications to each local DPA, nor will it be a requirement to notify or obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be broader internal record keeping requirements, as summarised below. A DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. In the new regulations, the DPO should meet the following requirements.

- Must be appointed based on professional qualities and, in particular, expert knowledge of data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could result in a conflict of interest



Some headlines of GDPR rules

- All organisations affected (meaning all organisations that control or process personal data on or about EU residents, including those based outside Europe) must develop both a technical and organisational capability prior to May 2018.Personal data is defined as any information relating to an identified or identifiable natural person, where identifiers include: name, ID number, email address, physical address, mental state, culture, religion, colour or anything else perceived to point to a specific identity.

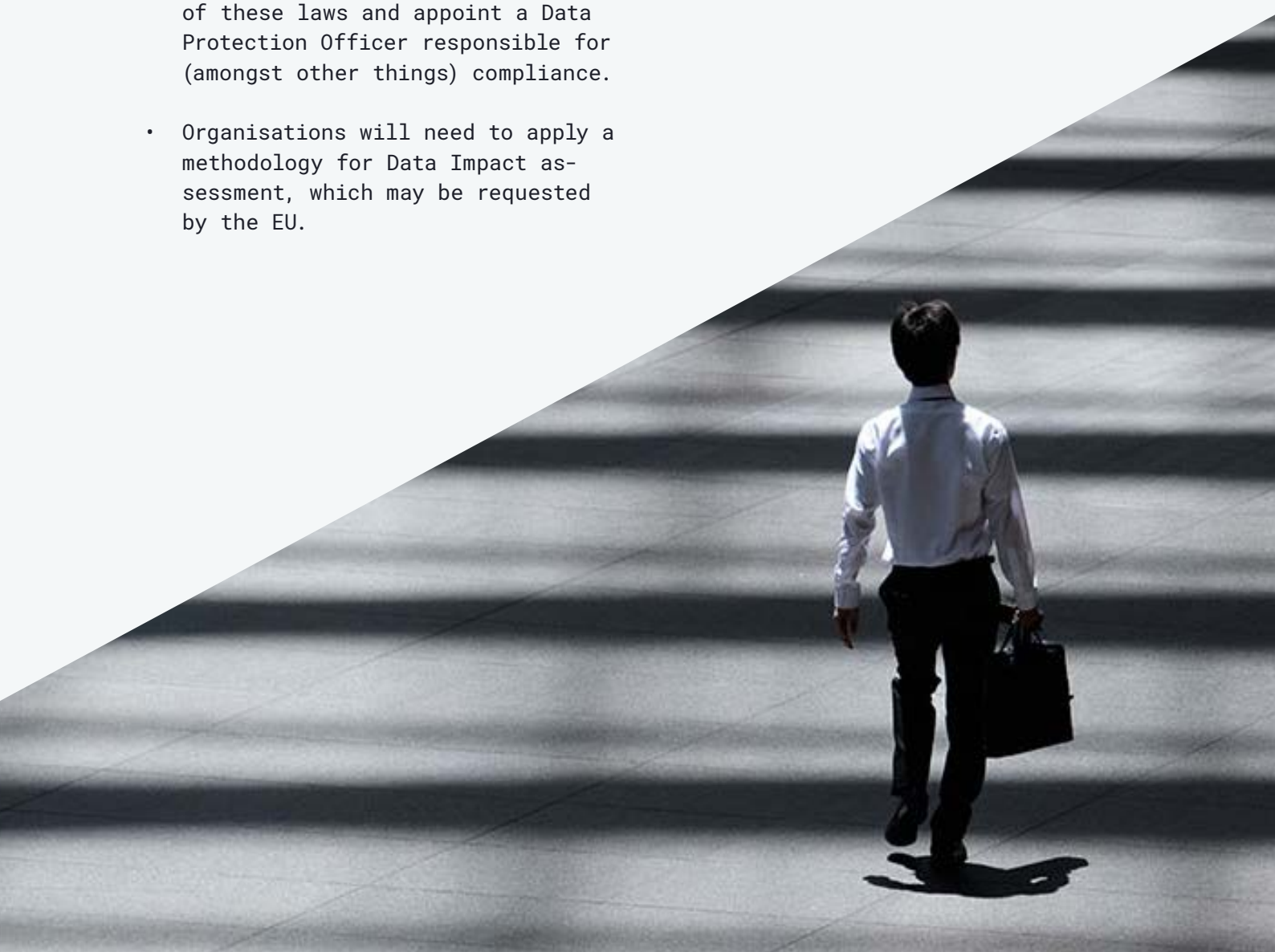
- All organisations affected will need to gain a clear and detailed understanding of the impact of these laws and appoint a Data Protection Officer responsible for (amongst other things) compliance.

- Organisations will need to apply a methodology for Data Impact assessment, which may be requested by the EU.

- Organisational demands include creation of policies for handling personal and sensitive data. Training staff in these policies is considered mandatory.

- Automated decision making and profiling may become much more restricted to ensure individual rights are not compromised by algorithm based analysis.

- The new GDPR rules were released in May 2016 and become law in May 2018.



How prepared are organisations for these changes?

Research shows widely different levels of preparation of organisations, with some industries doing better than others. The short summary below gives a flavour of the scale of readiness.

In general, European companies have a plan and understand the requirements.

Well, you would expect this, wouldn't you? Perhaps not, many European companies have had to make fast decisions on what they could, might and should do, as in the absence of meaningful penalties they have not worried about it too much. To balance this most EU countries have had long standing rules in place, the threat of greater penalties is catalysing action.

UK companies, and Local Government are well prepared.

The UK has been quite stringent in implementing data protection laws, with severe penalties being issued by a Government body, the Information Commissioners Office (ICO) for the last five years. Local Government in particular is attempting to be ready, but austerity measures and Brexit are leading to some conflict over the priority of actions.

US Companies with EU based customers are aware of the needs and demands but struggling with the apparent complexity of the laws.

Many US companies have small or no customer interaction with the EU, that they are aware of, but most have some level of need, and certainly have ambitions outside the US. So, will this inhibit US companies? Probably not. Will they be more likely to make mistakes? Probably not. Do they represent high profile candidates to catch out? For sure. A single very large fine, like Sony in the past draws attention to the rules and makes people act.

When surveyed, most companies claim some degree of readiness, few claim to be "fully prepared" meaning there is very much work in progress. Listed below are a number of questions asked. There are of course many more, and more emerge each day as hard pressed management teams look in ever greater detail at this.

What is the Scope of the regulation?

The regulation applies if the data controller or processor (organisation) or the data subject (person) is based in the EU. Furthermore, the Regulation also applies to organisations based outside the European Union if they process personal data of EU residents.

What kind of data is included?

According to the European Commission "personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address." The regulation does not apply to the processing of personal data for national security activities or law enforcement; however, the data protection reform package includes a separate Data Protection Directive for the police and criminal justice sector that provides robust rules on personal data exchanges at national, European and international level.

What is meant by a one-stop-shop?

Single set of rules and one-stop shop will apply to all EU member states. Each member state will establish an independent Supervisory Authority (SA) to hear and investigate complaints, sanction administrative offences, etc. SAs in each member state will cooperate with other SAs, providing mutual assistance and organising joint operations. Where a business has multiple establishments in the EU, it will have a single SA as its "lead authority", based on the location of its "main establishment" (i.e., the place where the main processing activities take place). The lead authority will act as a "one-stop shop" to supervise all the processing activities of that business throughout the EU (Articles 51 - 59 of the GDPR). A European Data Protection Board (EDPB) will coordinate the SAs. EDPB will replace the current conclusions of the under resourced Article 29 Working Party.

Are there any exceptions?

There are exceptions for data processed in an employment context and data processed for the purposes of national security, that still might be subject to individual country regulations (Articles 88 and 23 of the GDPR). However, the main bulk of data will relate to commercial activities within a market or Government related service.

Who is responsible and how are they held accountable?

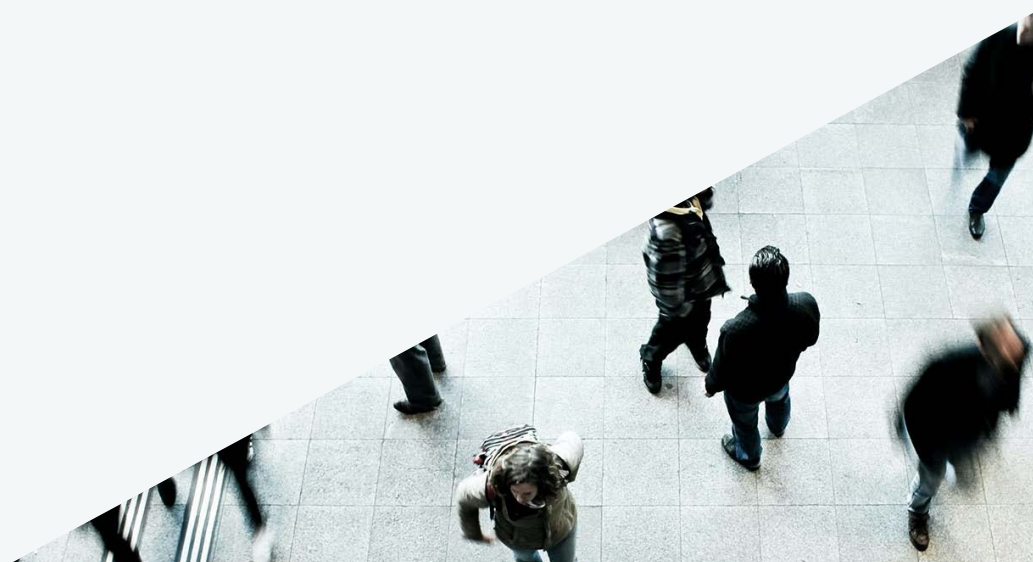
The existing notice requirements remain and are expanded. They must include the retention time for personal data and contact information for data controller and data protection officer has to be provided.

Automated individual decision-making, including profiling (Article 22) is made contestable. Citizens now have the right to question and fight decisions that affect them that have been made on a purely algorithmic basis.

Privacy by Design and by Default (Article 25) require that data protection is designed into the development of business processes for products and services.

Privacy settings must be set at a high level by default including for outbound email.

Data Protection Impact Assessments (Article 35) have to be conducted when specific risks occur to the rights and freedoms of data subjects. Risk assessment and mitigation is required and prior approval of the Data Protection Authorities (DPA) is required for high risks. Data Protection Officers (Articles 37–39) are to ensure compliance within organisations.



Data protection officers have to be appointed:

- for all public authorities, except for courts acting in their judicial capacity

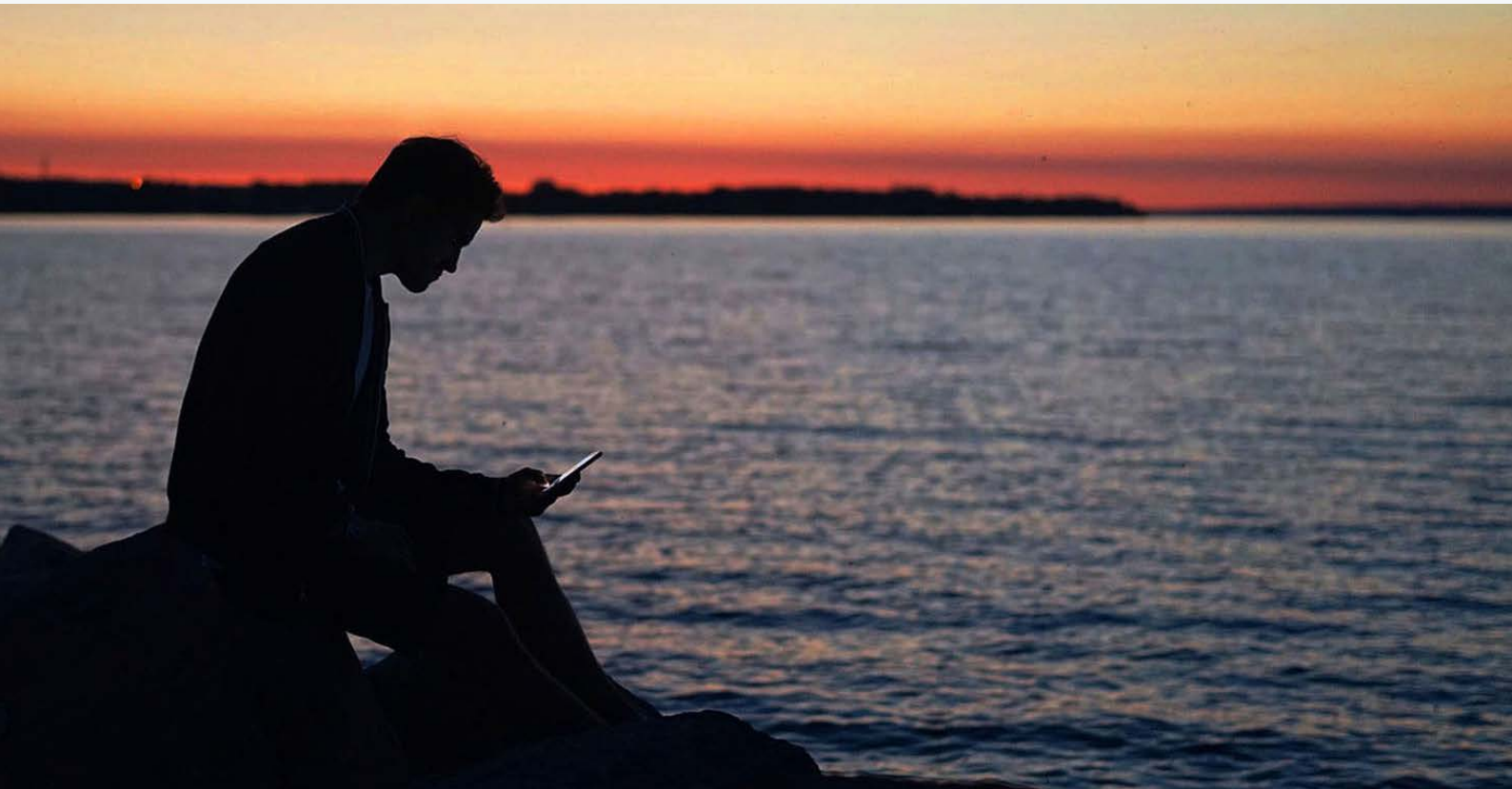
- if the core activities of the controller or the processor consist of:

  - processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale

  - processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10

What about consent?

Valid consent must be explicit for data collected and the purposes data is used for (Article 7; defined in Article 14). Consent for children must be given by the child's parent or custodian, and be verifiable (Article 8). Data controllers must be able to prove "consent" (opt-in) and consent may be withdrawn (opt out).

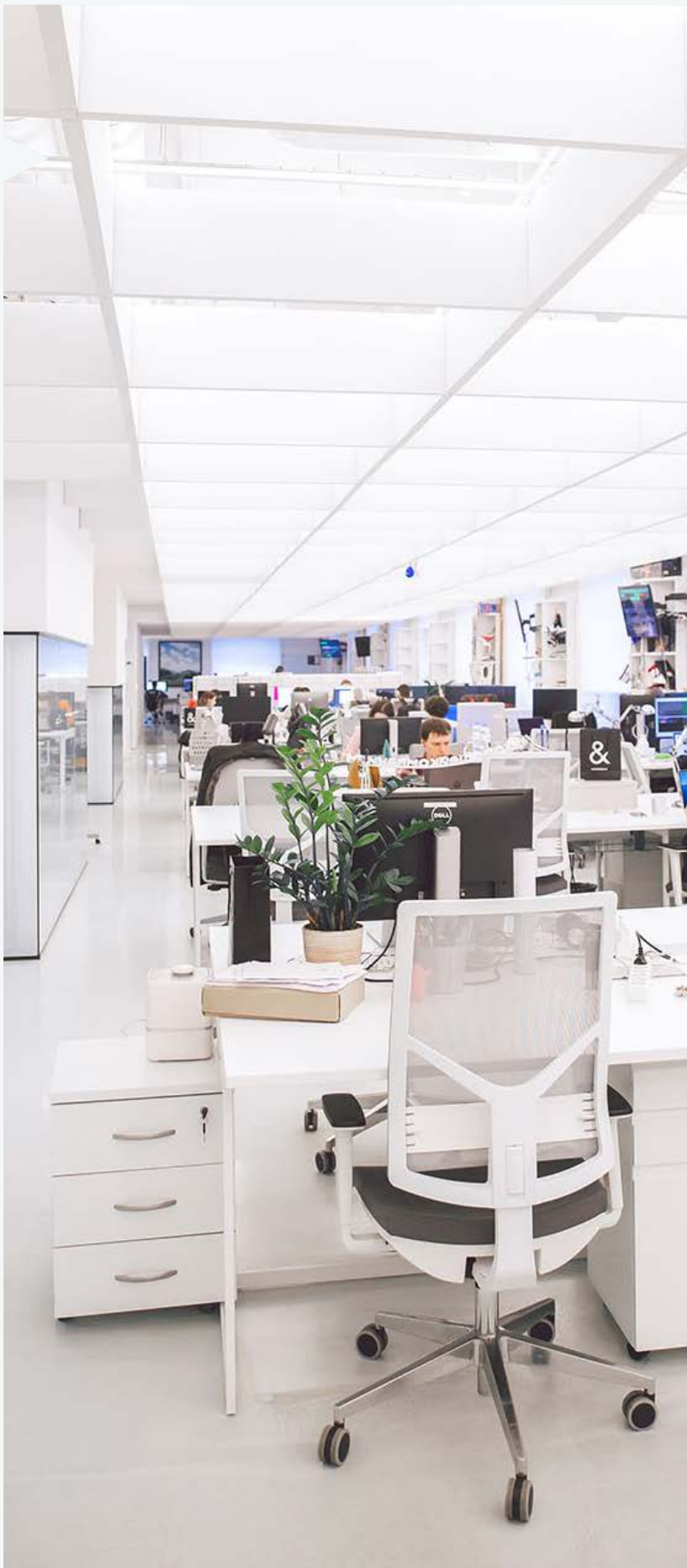


What is the role of the Data Protection Officer?

Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, or where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation.

The DPO is similar but not the same as a Compliance Officer as they are also expected to be proficient at managing IT processes, data security (including dealing with cyber-attacks) and other critical business continuity issues around the holding and processing of personal and sensitive data. The skill set required stretches beyond understanding legal compliance with data protection laws and regulations. This change is significant.

The appointment of a DPO within a large organisation will be a challenge for the Board as well as for the individual concerned. There are a myriad of governance and human factor issues that organisations and companies will need to address given the scope and nature of the appointment. In addition, the post holder will need to create their own support team and will also be responsible for their own continuing professional development as they need to be independent of the organisation that employs them, effectively as a “mini-regulator”.



What penalties and sanctions are likely?

The following sanctions can be imposed depending on severity of the breach:

- a warning in writing in cases of first and non-intentional non-compliance regular periodic data protection audits
- a fine up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (Article 83, Paragraph 4)
- a fine up to 20,000,000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (Article 83, Paragraphs 5 & 6)

How can we interpret the “Right to erasure”?

A so-called right to be forgotten was replaced by a more limited right to erasure in the version of the GDPR adopted by the European Parliament in March 2014. Article 17 provides that the data subject has the right to request erasure of personal data related to him on any one of a number of grounds including non-compliance with Article 6.1 (lawfulness) that includes a case where the legitimate interests of the controller is overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

This is controversial, especially when national security issues are in play, and we are in no doubt that many cases will be brought before the European Court of Human Rights (ECHR) before clear lines are established here.

How should we handle data portability requests?

A person should be able to transfer their personal data from one electronic processing system to and into another, without being prevented from doing so by the data controller. In addition, the data must be provided by the controller in a structured and commonly used electronic format.

The right to data portability is provided by Article 20 of the GDPR. Legal experts see in the final version of this measure a “new right” being created that “reaches beyond the scope of data portability between two controllers as stipulated in Article 18” although this point may need further clarification.

So what about technology to help handle these new demands?

Some good news first.

Most enterprises of any scale have an array of technology available (this may not be true for some smaller organisations) and have invested considerable sums in security solutions of one kind or another. One interviewee described 32 security solutions in various parts of the enterprise and these included:

- Data discovery, data cataloguing and data classification - user defined classification makes data handling more likely to comply with your rules. These technologies should be easy to use and be available at the point of decision by an individual that they will share information with others.
- Data Loss Prevention (DLP) catch data before it leaves the secure perimeter, but how do you scan encrypted data packages?
- Encryption of data at rest (whilst stored), back up once you know what you have in hand, but don't keep encrypted content for ever. For data at rest waiting to be used by another user or application you should apply strict data purging rules, especially where classified as including GDRP relevant items. Data should be purged in a controlled and policy driven manner so that no data graveyards develop.
- Archive solutions, archived data should be digitally signed so it can be fully authenticated allowing for non-repudiation.
- Encryption of data in use (in application) useful internally, but what about external users, or subjects? For encryption of email or data in transit use a unique key per transaction to limit the scope of any attack.
- Encryption of data in transit (both internally and externally when it leaves the security of your firewall). Many solutions miss out an ad hoc capability. Can you really force data subjects to comply with your key management demands? And be sure to avoid solutions where you have to manage user keys and credentials for all data subjects.

E-Mail-Verschlüsselung (PGP, S/MIME, Secure Email Gateways). Es ist Zeit ältere Technologien zu ersetzen, da sie nicht ad hoc verwendet werden können und weder mit großen Dateien umgehen noch Metadaten verschlüsseln können. Außerdem haben sie begrenzte oder keine Nachvollziehbarkeitsmöglichkeiten. Stellen Sie also sicher, dass Ihre E-Mail-Verschlüsselungstechnologie Ihnen detaillierte Nachvollziehbarkeitsmöglichkeiten aller Schritte, einschließlich Empfangsbestätigung, ermöglicht.

- Identifizieren und Verhindern von Datenverletzungen
- Sichere Datenübertragbarkeits-Möglichkeit. Wenn der Kunde eine Kopie von „allem“ ad hoc fordert, jetzt sofort
- Endpunktsicherheit und mobile Geräteverwaltung. Alte Technik in einer neuen Welt.
- Perimeter Sicherheit (letzte Verteidigungslinie). Gut verwaltet ist sie sehr effektiv aber auch sehr komplex und schnell kann etwas vergessen werden
- Speicher- und File-Sharing-Dienste in der Cloud lassen Fragen aufkommen über den Anbieter, den Grad an Sicherheit den sie erreichen, den Ort an dem die Daten gespeichert und als Back-up hinterlegt werden etc.
- Anti-Malware. Noch immer hauptsächlich Muster-basiert
- Anti-Spam. Phishing, noch immer reaktiv
- Sicherheit Penetration Tests und Compliance. Effektiv, aber wie oft können Sie es sich leisten, die Grenzen zu testen?
- Identitäts- und Zugriffsmanagement

Email encryption (PGP, S/MIME, Secure Email Gateways), older technology ripe to replace as they cannot be used ad hoc, don’t handle large files and don’t encrypt the very important meta data. In addition, they have limited if any audit trail so you should ensure your email encryption technology gives you a detailed audit trail of all steps along the way, including confirmation of receipt.

- Data breach identification and blocking, shutting the door after the horse has run.
- Secure data export capability, when the subject demands a copy of “everything” ad hoc, right now.
- Endpoint security and mobile device management, old tech in a new world.
- Perimeter security (last line of defence), well managed very effective, but complex and easy to miss things.
- Secure storage and sharing services in the cloud raises all kinds of questions about your supplier, the level of security they achieve, the location of data stored and backed up and so on.
- Anti-malware, still mainly pattern based
- Anti-spam, phishing, still reactive.
- Security penetration testing and compliance, effective but how often can you afford to test the boundary?
- Identity and access management.

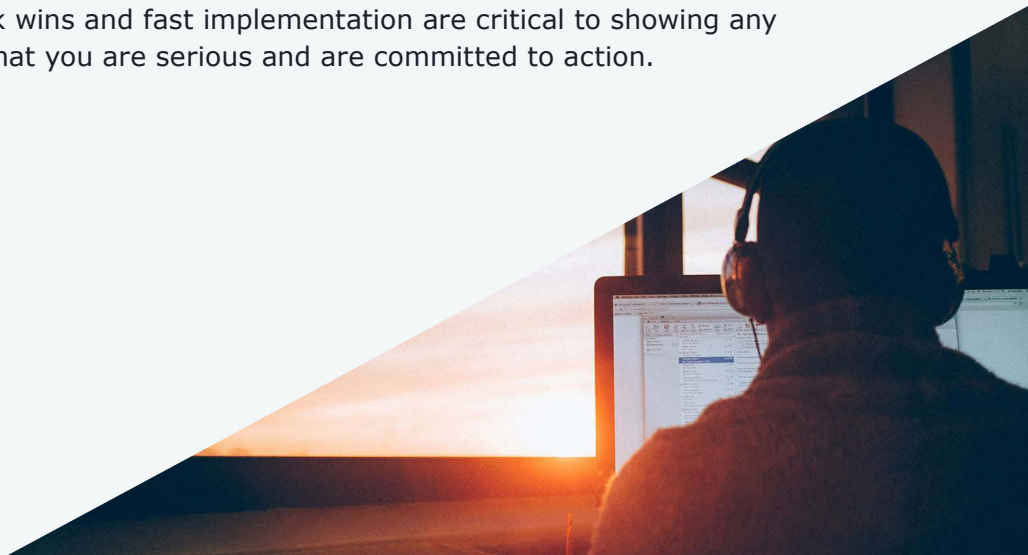
Some of the older legacy solutions are ripe to replace, so any kind of FTP, SFTP service should be replaced. S/Mime and PGP email encryption technologies leave your large files vulnerable and present barriers to ad hoc need, these can be replaced.

Shadow IT solutions (Dropbox, uSend IT, and so on) should be blocked with a secure configurable service offered in place of them.

Now the bad news.

You will need to find budget to make enhancements to your security systems, but by retiring legacy solutions you can perhaps end up saving money.

You need to action soon; quick wins and fast implementation are critical to showing any external observer or auditor that you are serious and are committed to action.



Pointsharp is a European cybersecurity company that enables organizations to secure data, identities and access in a user-friendly way. Because we believe easy to use security solutions lay the foundation for a modern digital workplace.

We deliver European made software and services that are made to support even the highest security and regulatory demands of large enterprise organizations and governmental institutions.

Our customers can be all around the world, often in markets requiring extra high levels of security, like the financial, governmental, industrial and defense sectors.

You can find our HQ in Stockholm, Sweden but we also have offices in Germany and the Netherlands.

Pointsharp – Security made easy

Visit our website for more information or a demo

wwww.pointsharp.com

POINTSHARP