TABLE OF CONTENTS

24. MAIN COUNTRIES AFFECTED BY THE GDPR
25. HOW THE GDPR WILL AFFECT NON-EU NATIONS?
    - Transferring Data Outside of the EU
    - GDPR versus Big Data
26. GDPR KEY CHANGES
    - Increased Territorial Scope (extraterritorial applicability)
    - Penalties
    - Consent
    - Data Subject Rights
    - Right to Access
    - Right to be forgotten
    - Data Portability
    - Privacy by Design
    - Data protection officers
27. THE 8 BASIC DATA PROTECTION RIGHTS OF GDPR FOR CUSTOMERS
28. IMPACTS ON THE FINANCIAL INDUSTRY UNDER GDPR
29. IMPACT ON BANKING SECTOR
30. HOW BANKS SHOULD PREPARE FOR THE GDPR
    - Documenting a lawful basis for processing
    - Hire a DPO
    - Prepare for the right to data portability
31. THE IMPACT OF GDPR ON CUSTOMER ENGAGEMENT
32. KEY CHALLENGES ASSOCIATED WITH THE GDPR
    - Many new requirements
    - Very process-driven
    - Very tangible and visible/verifiable functions and steps need to berealized
    - Increased fines and sanctions
33. FUTURE OPPORTUNITIES
34. FIVE BENEFITS GDPR COMPLIANCE WILL BRING TO YOUR BUSINESS
    - Benefit One: Enhance Your Cyber security
    - Benefit Two: Improve Data Management
    - Benefit Three: Increase Marketing Return On Investment (ROI)
    - Benefit Four: Boost Audience Loyalty And Trust
    - Benefit Five: Become the First To Establish A New Business Culture
35. The Ten Key Issues Businesses Should Understand While Making Themselves GDPR Compliant
    - Most stuff is changing, however not the entire thing
    - A DPO should be designated

- The introduction of mandatory Privacy Impact Assessments (PIAs)
- Data subjects rights
- Geographic application
- Notifying a data breach within 72 hours
- Fines
- Consent
- Compliance obligations for controllers to be increased
- Direct compliance obligations for processors

36. UNEXPECTED CONSEQUENCES OF GDPR
    - Restriction of Privacy and Innovation
    - Road blocks For Block chain Data Storage
    - Opt-In Fatigue
    - Poor Customer Service
    - Small Businesses Getting Hurt
    - The Slow Death of Free Services
    - Talk About Similar Regulation In The U.S.
    - Photography Being Part of GDPR
    - C-Suite Becoming Responsible For Data Security
    - Restricted Technology Access for EU Citizens
    - Reduced Ability To Track Cybercrime
    - More Meaningful Customer Engagement
    - Country Legislation At Odds With GDPR
    - U.S. Websites Denying Access To EU Visitors
    - Increased Value of First-Party Data
37. THE POSITIVE AND NEGATIVE IMPLICATIONS OF GDPR

    The Positive Implications of GDPR

    - Improved Cybersecurity
    - Standardization of Data Protection
    - Brand Safety
    - Loyal Customer Following

    The Negative Implications of GDPR

    - Non-Compliance Penalties
    - The Cost of Compliance
    - Overregulation
    - The Aftermath of Implementation
38. FREQUENTLY ASKED QUESTIONS
39. REFERENCES
40. ARTICLES

General Data Protection Regulation

A BRIEF HISTORY

The **GDPR** will take effect in May 2018. To better understand these new data privacy reforms, this article will analyse its background.

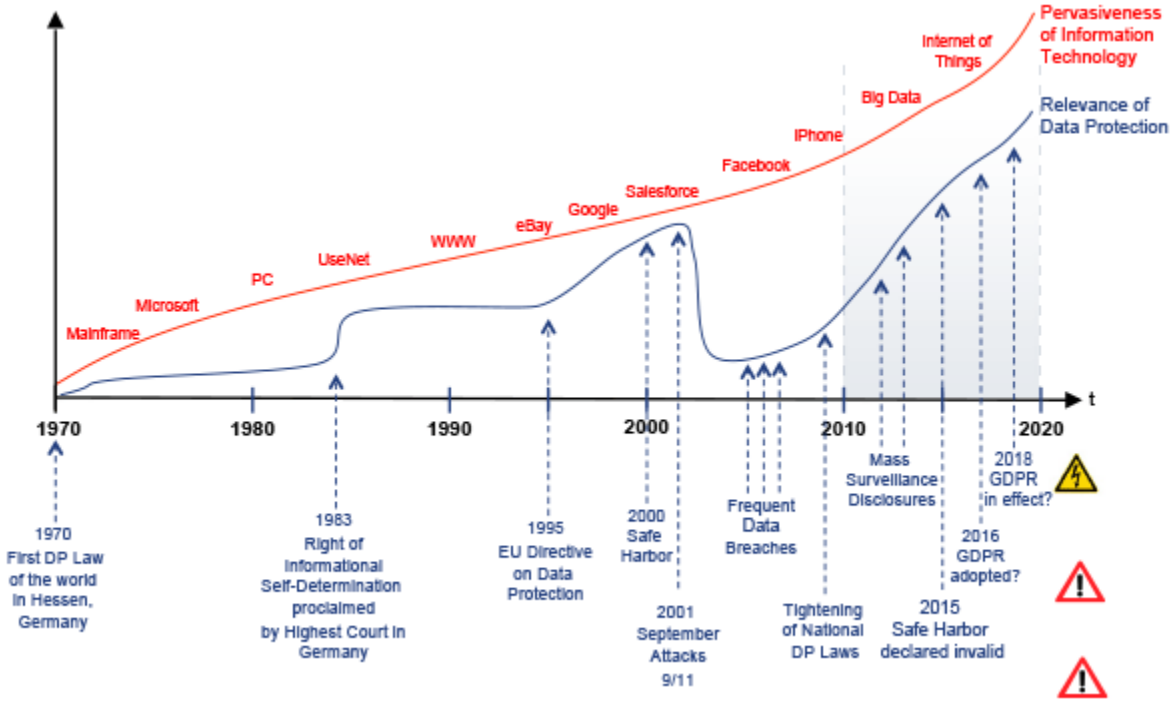
Back in 1950, the basic principles of data protection were set y the EU convention on human rights. This stated everyone should have had their privacy protected unless legal or security reasons were involved.

The technological revolution in the 80s saw the increased use of computers and changed enormously the way data were collected, processed and stored. It is during these years that a stronger control over data became imperative. In 1995, in order to be more rigorous about data protection, the European Data Protection Directive was adopted. The directive set a number of minimum requirements which had to be followed by the member states. This inspired the development of the Data Protection Act 1998 in the UK.

In the subsequent years, the online panorama kept evolving at unprecedented pace causing, in 2012, the European Commission to propose a reform of the EU's 1995 data protection rules in order to enhance online safety. In this year, concerns regarding

privacy grew, giving a start to a series of debates. In the same year, the Article 29 Working Party updated the European Commission reform proposal, providing their opinion and highlighting areas of concern.

In March 2014, the European Parliament reached an agreement and the new data protection reform, the GDPR, voted in plenary with 621 votes in favour became irreversible. In 2016 the GDPR enters into force giving members two years to ensure it is fully implementable in their countries by 25th May 2018. [1]



TIMELINE

- 25 January 2012: The proposal for the GDPR was released.
- 21 October 2013: The European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) had its orientation vote.
- 15 December 2015: Negotiations between the European Parliament, Council and Commission (Formal Trilogue meeting) resulted in a joint proposal.
- 17 December 2015: The European Parliament's LIBE Committee voted for the negotiations between the three parties.

- 8 April 2016: Adoption by the Council of the European Union. The only member state voting against was Austria, which argued that the level of data protection in some respects falls short compared to the 1995 directive.
- 14 April 2016: Adoption by the European Parliament[
- 24 May 2016: The regulation entered into force, 20 days after its publication in the *Official Journal of the European Union*.
- 25 May 2018: Its provisions became directly applicable in all member states, two years after the regulations enter into force.
- 20 July 2018: the GDPR became valid in the EEA countries (Iceland, Liechtenstein, and Norway) after the EEA Joint Committee and the three countries agreed to follow the regulation.

OVERVIEW

The GDPR has been under discussion within the EU, since 2012 and is an update to existing data protection-related legislation. The final, official summary outlining GDPR, is as follows:

"The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies"

It's clear that the reasoning behind GDPR is to protect EU citizens' personal data in a way that is transparent and measurable. But, for many businesses, this will require significant changes to the way they manage and store their customer data.

Whenever a new rule that will affect a major part of the infrastructure of your business systems is required, it can seem like a huge headache you wish you could get rid of. The only way to remove any GDPR concerns is to ensure your business is compliant to all the relevant new rules when they come into force by the date of enforcement.

Luckily for small businesses, there are a few exemptions which have been designed to ensure smaller, often less wealthy businesses, aren't bogged down by masses of expensive requirements. While there are still many changes that *will* need to be made, fortunately, it's possible to adopt GDPR in a way that benefits your business as well as safeguarding your customer's personal data.

DEFINITION

The General Data Protection Regulation ("GDPR") is a legal framework that requires businesses to protect the personal data and privacy of European Union (EU) citizens for

transactions that occur within EU member states. It covers all companies that deal with the data of EU citizens, specifically banks, insurance companies, and other financial companies.

GDPR DATE

GDPR will apply across the European Union from 25 May 2018, and all member nations are expected to have transferred it into their own national law by 6 May 2018.

Following four years of preparation and debate, GDPR was approved by the European Parliament in April 2016 and the official texts and regulation of the directive were published in all of the official languages of the EU on May 2016.

GDPR comes into force on 25 May 2018.

GDPR compliance deadline:

As of 25 May 2018, all organisations are expected to be compliant with GDPR.

REAL PURPOSE OF THE GDPR

The purpose of the GDPR is to provide a set of standardized data protection laws across all the member countries. This should make it easier for EU citizens to understand how their data is being used, and also raise any complaints, even if they are not in the country where its located.

Despite the UK's exit from the EU it is still expected to affect British businesses (GDPR and Brexit for more info).

STRUCTURE

The GDPR consists of 99 *articles*, grouped into 11 chapters, and an additional 171 *recitals* with explanatory remarks. The chapters' headings are:

I - General provisions

II - Principles

III - Rights of the data subject

IV - Controller and processor

V - Transfers of personal data to third countries or international organizations

VI - Independent supervisory authorities

VII - Cooperation and consistency

VIII - Remedies, liability and penalties

IX - Provisions relating to specific processing situations

X - Delegated acts and implementing acts

XI - Final provisions

SCOPE

The regulation applies if the data controller (an organisation that collects data from EU residents), or processor (an organisation that processes data on behalf of a data controller like cloud service providers), or the data subject (person) is based in the EU. Under certain circumstances, the regulation also applies to organisations based outside the EU if they collect or process personal data of individuals located inside the EU. The regulation does not apply to the processing of data by a person for a "purely personal or household activity and thus with no connection to a professional or commercial activity." (Recital 18)

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 home address, a photo, an email address, bank details, posts on social networking websites,, medical information, or a computer's IP address. The precise definitions of terms such as "personal data", "processing", "data subject", "controller" and "processor", are stated in Article 4 of the Regulation.

The regulation does not purport to apply to the processing of personal data for national security activities or law enforcement of the EU; however, industry groups concerned about facing a potential conflict of laws have questioned whether Article 48 of the GDPR could be invoked to seek to prevent a data controller subject to a third country's laws from complying with a legal order from that country's law enforcement, judicial, or national security authorities to disclose to such authorities the personal data of an EU person, regardless of whether the data resides in or out of the EU. Article 48 states that any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may not be recognised or enforceable in any manner unless based on an international agreement, like a mutual legal assistance treaty in force between the requesting third (non-EU) country and the EU or a member state. The data protection reform package also includes a separate Data Protection Directive for the police and criminal justice sector that provides rules on personal data exchanges at national, European, and international levels.

A single set of rules 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 co-operate with other SAs, providing mutual assistance and organising joint operations. If 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" 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 46–55 of the GDPR). A European Data Protection Board (EDPB) will co-ordinate the SAs. EDPB will replace the Article 29 Data Protection Working Party. There are exceptions for data processed in an employment context or in national security that still might be subject to individual country regulations (Articles 2(2)(a) and 88 of the GDPR).

LAWFUL BASIS FOR PROCESSING

Unless a data subject has provided informed consent to data processing for one or more purposes, personal data may not be processed unless there is at least one legal basis to do so. According to Article 6, the lawful purposes are:

- If the data subject has given consent to the processing of his or her personal data;
- To fulfill contractual obligations with a data subject, or for tasks at the request of a data subject who is in the process of entering into a contract;
- To comply with a data controller's legal obligations;
- To protect the vital interests of a data subject or another individual;

- To perform a task in the public interest or in official authority;
- For the legitimate interests of a data controller or a third party, unless these interests are overridden by interests of the data subject or her or his rights according to the Charter of Fundamental Rights (especially in the case of children).

If informed consent is used as the lawful basis for processing, consent must have been explicit for data collected and each purpose data is used for (Article 7; defined in Article 4). Consent must be a specific, freely-given, plainly-worded, and unambiguous affirmation given by the data subject; an online form which has consent options structured as an opt-out selected by default is a violation of the GDPR, as the consent is not unambiguously affirmed by the user. In addition, multiple types of processing may not be "bundled" together into a single affirmation prompt, as this is not specific to each use of data, and the individual permissions are not freely-given. (Recital 32)

Data subjects must be allowed to withdraw this consent at any time, and this process must be as easy as it was to originally opt in. (Article 7(3)) A data controller may not refuse service to users who decline consent to processing that is not strictly necessary in order to use the service. (Article 7(4)) Consent for children, defined in the regulation as being less than 16 years old (although with the option for member states to individually make it as low as 13 years old (Article 8(1)), must be given by the child's parent or custodian, and verifiable (Article 8).

If consent to processing was already provided under the Data Protection Directive, a data controller does not have to re-obtain consent if the processing is documented and obtained in compliance with the GDPR's requirements (Recital 171).

ACCOUNTABILITY AND COMPLIANCE

Companies covered by the GDPR are accountable for their handling of people's personal information. This can include having data protection policies, data protection impact assessments and having relevant documents on how data is processed.

In recent years, there have been a score of massive data breaches, including millions of Yahoo, LinkedIn, and MySpace account details. Under GDPR, the "destruction, loss, alteration, unauthorised disclosure of, or access to" people's data has to be reported to a country's data protection regulator where it could have a detrimental impact on those who it is about. This can include, but isn't limited to, financial loss, confidentiality breaches, damage to reputation and more. The ICO has to be told about a breach 72 hours after an organisation finds out about it and the people it impacts also need to be told.

For companies that have more than 250 employees, there's a need to have documentation of why people's information is being collected and processed, descriptions of the information that's held, how long it's being kept for and descriptions of technical security measures in place.

Additionally, companies that have "regular and systematic monitoring" of individuals at a large scale or process a lot of sensitive personal data have to employ a data protection officer (DPO). For many organisations covered by GDPR, this may mean having to hire a new member of staff – although larger businesses and public authorities may already have people in this role. In this job, the person has to report to senior members of staff, monitor compliance with GDPR and be a point of contact for employees and customers. "It means the data protection will be a boardroom issue in a way it hasn't in the past combined," Denham says.

There's also a requirement for businesses to obtain consent to process data in some situations. When an organisation is relying on consent to lawfully use a person's information they have to clearly explain that consent is being given and there has to be a "positive opt-in". A blog post from Denham explains there are multiple ways for organisations to process people's data that doesn't rely upon consent.

DATA PROTECTION BY DESIGN AND BY DEFAULT

Data protection by design and by default (Article 25) requires data protection to be designed into the development of business processes for products and services. Privacy settings must therefore be set at a high level by default, and technical and procedural measures should be taken by the controller to make sure that the processing, throughout the whole processing lifecycle, complies with the regulation. Controllers should also implement mechanisms to ensure that personal data is not processed unless necessary for each specific purpose.

A report by the European Union Agency for Network and Information Security elaborates on what needs to be done to achieve privacy and data protection by default. It specifies that encryption and decryption operations must be carried out locally, not by remote service, because both keys and data must remain in the power of the data owner if any privacy is to be achieved. The report specifies that outsourced data storage on remote clouds is practical and relatively safe if only the data owner, not the cloud service, holds the decryption keys.

B2B MARKETING

Within the GDPR there is a distinct difference between business to consumer (B2C) and business to business (B2B) marketing. Under the GDPR, there are six equally valid

grounds to process personal data. There are two of these which are relevant to direct B2B marketing; they are *consent* or *legitimate interest*. Recital 47 of the GDPR states that "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

Using *legitimate interest* as the basis for B2B marketing involves ensuring key conditions are met:

"The processing must relate to the legitimate interests of your business or a specified third party, providing that the interests or fundamental rights of the data subject do not override the business' legitimate interest."

"The processing must be necessary to achieve the legitimate interests of the organisation."

Additionally, Article 6.1(f) of the GDPR states that the processing is lawful if it is "Necessary for the purposes of the legitimate interests pursued by the controller or by a third-party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual which require protection of personal information, in particular where the individual is a child".

Therefore, companies can continue to use marketing data for the purposes of B2B engagement as long as the appropriate steps are taken to ensure the data is aligned to a specific objective or campaign. One phrase that is now being used is "Correct Marketing to the Correct Person". As part of this companies will need to keep their marketing databases and CRM up to date in order to carry out valid Legitimate Balance Checks.

The EU Commission stated that, "Unified data privacy laws will create extraordinary opportunities and motivating innovation for businesses not only within Europe but also for the organization who are willing to do business with European states or already running their business in European states." The commission aims for companies to maintain communications and build regulation supporting relationships with each other to ensure best data practices through *legitimate balance checks*.[

ACCESS TO YOUR DATA

as well putting new obligations on the companies and organisations collecting personal data, the gdpr also gives individuals a lot more power to access the information that's held about them.

A subject access request (SAR) allows an individual the ability to ask a company or organisation to provide data about them. Previously, these requests cost £10 but gdpr

scraps the cost and makes it free to ask for your information. When someone makes a sar businesses must stump up the information within one month. Everyone will have the right to get confirmation that an organisation has information about them, access to this information and any other supplementary information. As dixon points out, big technology companies, as well as smaller startups, will have to give users more control over their data.

as well as this the gdpr bolsters a person's rights around automated processing of data. The icon says individuals "have the right not to be subject to a decision" if it is automatic and it produces a significant effect on a person. there are certain exceptions but generally people must be provided with an explanation of a decision made about them.

The regulation also gives individuals the power to get their personal data erased in some circumstances. this includes where it is no longer necessary for the purpose it was collected, if consent is withdrawn, there's no legitimate interest, and if it was unlawfully processed.

THE 1995 DATA PROTECTION DIRECTIVE

In April 2016, the European Parliament adopted the GDPR, replacing its outdated Data Protection Directive, enacted back in 1995. Unlike a regulation, a directive allows for each of the twenty-eight members of the EU to adopt and customize the law to the needs of its citizens, whereas a regulation requires its full adoption with no leeway by all 28 countries second. In this instance, the GDPR requires all 28 countries of the EU to comply.

The issue with the Directive is that it's no longer relevant to today’s digital age. Its provisions fail to address how data is stored, collected, and transferred today—a digital age. Like many regulations and statutes throughout the EU and U.S., these regulations haven’t been able to keep up with the pace of the levels of technological advancement.

The full text of GDPR is comprised of 99 articles, setting out the rights of individuals and obligations placed on businesses that are subject to the regulation. GDPR’s provisions also require that any personal data exported outside the EU is protected and regulated. In other words, if any European citizen's data is touched, you better be compliant with the GDPR. For example, a U.S. airline is selling services to someone out in the UK, although the airline is located in the U.S., they are still required to comply with GDPR because of the European data being involved.

It is a very high standard to meet, requiring that companies invest large sums of money to ensure they are in compliance. According to the EU’s GDPR website, the legislation is designed to “harmonize” data privacy laws across Europe, providing greater protection and rights to individuals.

Before the Internet, Europe has long been the model for how our data should be protected and regulated. The reason is that the public's concern over privacy has dominated the business sphere, ensuring that a stringent rule on how companies use the personal data of its citizens is always taken into account.

Two days ago, the UK government created and enacted a new Data Protection Act, replacing the previous law that was passed into law back in 1998. Running 353 pages and full of complex provisions, it largely incorporates all the provisions of GDPR, but differs in that individual countries were able to select parts of GDPR that could be customized to their citizen's needs.

After months of learning about data breaches from companies like Facebook and Equifax, this couldn't be more necessary. Even Mark Zuckerberg's jumped on board in his testimony before Congress on Capitol Hill, believing GDPR to be a very positive step for the Internet.

WHAT DATA IS PROTECTED UNDER GDPR?

With the enactment of GDPR today, two major protective rights should be highlighted. First the right to assure, or the right to be forgotten. If you don't want your data out there, then you have the right to request for its removal or erasure. Second, the right of portability. When it comes to "opt-in/opt-out" clauses, the notices to users must be very clear and precise as to its terms.

GDPR requires clear consent and justification. Pursuant to the GDPR, the following types of data is addressed and covered:

- Personally identifiable information, including names, addresses, date of births, social security numbers
- Web-based data, including user location, IP address, cookies, and RFID tags
- Health (HIPAA) and genetic data
- Biometric data
- Racial and/or ethnic data
- Political opinions
- Sexual orientation

THE GDPR: UNDERSTANDING THE 6 DATA PROTECTION PRINCIPLES

The EU General Data Protection Regulation (GDPR) outlines six data protection principles that organisations need to follow when collecting, processing and storing individuals' personal data. The data controller is responsible for complying with the principles and must be able to demonstrate the organisation's compliance practices.

We've listed the six principles here with advice on how you can follow them.

Lawfulness, fairness and transparency

The first principle is relatively self-evident: organisations need to make sure their data collection practices don't break the law and that they aren't hiding anything from data subjects.

To remain lawful, you need to have a thorough understanding of the GDPR and its rules for data collection. To remain transparent with data subjects, you should state in your privacy policy the type of data you collect and the reason you're collecting it.

Purpose limitation

Organisations should only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose.

Processing that's done for archiving purposes in the public interest or for scientific, historical or statistical purposes is given more freedom.

Data minimization

Organisations must only process the personal data that they need to achieve its processing purposes. Doing so has two major benefits. First, in the event of a data breach, the unauthorised individual will only have access to a limited amount of data. Second, data minimization makes it easier to keep data accurate and up to date.

Accuracy

The accuracy of personal data is integral to data protection. The GDPR states that "every reasonable step must be taken" to erase or rectify data that is inaccurate or incomplete.

Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days.

Storage limitation

Similarly, organisations need to delete personal data when it's no longer necessary.

How do you know when information is no longer necessary? According to marketing company Epsilon Abacus, organisations might argue that they "should be allowed to store the data for as long as the individual can be considered a customer. So the question really is: For how long after completing a purchase can the individual be considered a customer?"

The answer to this will vary between industries and the reasons that data is collected. Any organisation that is uncertain how long it should keep personal data should consult a legal professional.

Integrity and confidentiality

This is the only principle that deals explicitly with security. The GDPR states that personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures".

The GDPR is deliberately vague about what measures organisations should take, because technological and organizational best practices are constantly changing. Currently, organisations should encrypt and/or pseudonymise personal data wherever possible, but they should also consider whatever other options are suitable.

GDPR TRAINING

These six principles provide an overview of the areas covered in the GDPR, but they are far from comprehensive. The rest of the Regulation goes into much more detail on the specific practices that organisations should undertake to make sure they remain compliant.

Those who want to learn more about the GDPR should consider enrolling on our Certified EU General Data Protection Regulation Foundation (GDPR) Training Course.

This one-day course is the perfect introduction to the GDPR and the requirements you need to meet. It's delivered by an experienced data protection practitioner, and is suitable for directors or managers who want to understand how the GDPR affects their organisation, employees who are responsible for GDPR compliance and those with a basic knowledge of data protection who want to develop their career.

KEY PROVISIONS OF THE GDPR

GDPR compliance is something that the biggest companies in the world are currently grappling with, and will likely grapple with up until the deadline on May 25th, 2018 (and maybe even beyond).

Even if we distill GDPR compliance down to the basics, there are a lot of requirements you'll have to implement to make sure you're in line. Here's what you should start thinking about:

1. Obtaining consent

Your terms of consent must be clear. This means that you can't stuff your terms and conditions with complex language designed to confuse your users. Consent must be easily given and freely withdrawn at any time.

2. Timely breach notification

If a security breach occurs, you have 72 hours to report the data breach to both your customers and any data controllers, if your company is large enough to require a GDPR data controller. Failure to report breaches within this timeframe will lead to fines.

3. Right to data access

If your users request their existing data profile, you must be able to serve them with a fully detailed and free electronic copy of the data you've collected about them. This report must also include the various ways you're using their information.

4. Right to be forgotten

Also known as the right to data deletion, once the original purpose or use of the customer data has been realized, your customers have the right to request that you totally erase their personal data.

5. Data portability

This gives users rights to their own data. They must be able to obtain their data from you and reuse that same data in different environments outside of your company.

6. Privacy by design

This section of GDPR requires companies to design their systems with the proper security protocols in place from the start. Failure to design your systems of data collection the right way will result in a fine.

7. Potential data protection officers

In some cases, your company may need to appoint a data protection officer (DPO). Whether or not you need an officer depends upon the size of your company and at what level you currently process and collect data.

REQUIREMENTS OF GENERAL DATA PROTECTION REGULATION 2018

The GDPR itself contains 11 chapters and 91 articles. The following are some of the chapters and articles that have the greatest potential impact on security operations:

- Articles 17 & 18 – Articles 17 and 18 of the GDPR give data subjects more control over personal data that is processed automatically. The result is that data subjects may transfer their personal data between service providers more easily (also called the “right to portability”), and they may direct a controller to erase their personal data under certain circumstances (also called the “right to erasure”).
- Articles 23 & 30 – Articles 23 and 30 require companies to implement reasonable data protection measures to protect consumers’ personal data and privacy against loss or exposure.
- Articles 31 & 32 – Data breach notifications play a large role in the GDPR text. Article 31 specifies requirements for single data breaches: controllers must notify SAs of a personal data breach within 72 hours of learning of the breach and must provide specific details of the breach such as the nature of it and the approximate number of data subjects affected. Article 32 requires data controllers to notify data subjects as quickly as possible of breaches when the breaches place their rights and freedoms at high risk.
- Articles 33 & 33a – Articles 33 and 33a require companies to perform Data Protection Impact Assessments to identify risks to consumer data and Data Protection Compliance Reviews to ensure those risks are addressed.
- Article 35 – Article 35 requires that certain companies appoint data protection officers. Specifically, any company that processes data revealing a subject’s genetic data, health, racial or ethnic origin, religious beliefs, etc. must designate a data protection officer; these officers serve to advise companies about compliance with the regulation and act as a point of contact with Supervising Authorities (SAs). Some companies may be subjected to this aspect of the GDPR simply because they collect personal information about their employees as part of human resources processes.

- Articles 36 & 37 – Articles 36 and 37 outline the data protection officer position and its responsibilities in ensuring GDPR compliance as well as reporting to Supervisory Authorities and data subjects.
- Article 45 – Article 45 extends data protection requirements to international companies that collect or process EU citizens' personal data, subjecting them to the same requirements and penalties as EU-based companies.
- Article 79 – Article 79 outlines the penalties for GDPR non-compliance, which can be up to 4% of the violating company's global annual revenue depending on the nature of the violation.

WHO IS SUBJECT TO GDPR COMPLIANCE?

The purpose of the GDPR is to impose a uniform data security law on all EU members, so that each member state no longer needs to write its own data protection laws and laws are consistent across the entire EU. In addition to EU members, it is important to note that any company that markets goods or services to EU residents, regardless of its location, is subject to the regulation. As a result, GDPR will have an impact on data protection requirements globally.

PENALTIES FOR NONCOMPLIANCE WITH THE GDPR

Penalties for failing to comply with the provisions of the GDPR can be severe and carry significant risk of liability for any company. The maximum assessable penalty for noncompliance with the GDPR is 4% of the annual global revenue generated by the company. The maximum penalty will be imposed on organizations failing to acquire sufficient customer consent to process data or for violating the Privacy by Design concept.

Other violations are assessed on a tiered basis depending on the infraction. For example, a company can be fined 2% for not having its records in order, not notifying the supervising authority and the data subject about a security breach in a timely manner, or for not conducting a required impact assessment of a security breach.

GDPR DATA BREACH NOTIFICATION

GDPR data breach notification requirements mark a noticeable change. Companies now have 72 hours to log the discovery of a data breach with the relevant data protection authorities.

It's important to remember that only data breaches which cause harm need be reported. For Data Processors this time only stands once they have discovered the breach.

Companies which fail to do so may find themselves facing additional fines.

THE FIRST GDPR INVESTIGATIONS

Since GDPR started to be enforced in May a number of investigations into new data breaches have started.

So far, the biggest data incident has been Facebook's admission that 50 million access tokens for its accounts were taken by unknown hackers. In Europe the Irish data protection commissioner has opened an investigation into the hack. The investigation is due to look at the technical and organizational measures Facebook had in place to protect customer data.

Elsewhere, the hack of British Airways has come under scrutiny from regulators. During August and September, hackers inside the airline's systems compromised the account data of 380,000 people. The incident is being looked at by the ICO.

Only data breaches that happened since the introduction of GPDR can be investigated under the law. If a data incident occurred before May 25 then penalties in the UK can only be applied under the Data Protection Act 1998.

MAIN COUNTRIES AFFECTED BY THE GDPR

As mentioned above, the physical location of the institution, organization or business is not as important in determining the need to comply with the GDPR as the physical location of the data subject – the individual whose data is being collected, processed or stored. We have stated already that most organizations will find themselves subject to or impacted by the GDPR. Organizations in the following countries, the EU member states, will probably be most affected by the GDPR:

- Austria
- Belgium
- Bulgaria
- Croatia
- Republic of Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland

- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- United Kingdom

As the United Kingdom will still be a member of the European Union when the GDPR comes into force, the regulation will be absorbed into the UK´s domestic law under Clause 3 of the European Union (Withdrawal) Bill. The UK government is also in the process of debating a new Data Protection Bill which is closely aligned to the GDPR with a few minor exceptions (for example the right of individuals to have all social media postings from their childhood deleted) and exemptions (for example exemption from the Data protection Bill for journalists and whistle-blowers in certain circumstances).

Other EU member states are also introducing their own national laws to compliment the introduction of the GDPR. Most of them closely match the privacy and security requirements of the GDPR and, where they deviate, the changes mostly concern the age of consent for children, the need to obtain employees´ consent before processing their data, minor restrictions on the Rights of Individuals, and an extension of “special categories” when it is in the public interest.

HOW THE GDPR WILL AFFECT NON-EU NATIONS?

The GDPR will have a global impact even with the relatively small and localized nature of the EU itself. Despite EU countries being more likely to see the most change, non-EU countries are likely to see greater disruption following the introduction of the GDPR. This is due to the fact that organizations located within the EU are more likely to be prepared for the changes as they as more likely to be aware of the introduction of the GDPR. A large number of organizations located outside of the EU are still unaware of the coming change or are of the opinion that they are exempt or will be unaffected.

There is also a sociological difference at play: non-EU societies such as the United States (US) and others do not have the same expectation of privacy as many EU societies. Privacy laws are in place for certain types of “sensitive” data, such as the Health Insurance Portability and Accountability Act (HIPAA), which regulates healthcare information; or the Gramm-Leach-Bliley Act, which concerns financial information; but “general” data does not enjoy the same protections. For this reason, only US-based organizations and businesses that have Privacy Shield certification will be able to migrate dat from the EU.

The need to implement, staff, and run parallel systems may introduce too much complexity and drive costs too high for US-based organizations and businesses to continue offering their services to the EU market. A potential strategy may be for US-based actors to adopt an “all or nothing” approach that protects “general” data in a way currently reserved for “sensitive” data. This may allow the same system to be used to comply with both HIPAA, for example, and the GDPR. As of now, it is unclear whether many US groups will attempt this strategy.

Transferring Data Outside of the EU

The GDPR places strict controls on data transferred to non-EU countries or international organizations. These are detailed in Chapter V of the Regulation. Data is allowed to be transferred only when the EU Commission has deemed that the transfer destination “ensures an adequate level of protection”.

Data transfers can also occur in situations where the receiving entity can demonstrate that they meet this “adequate level of protection”, subject to periodic review every four years. The necessary protections may include:

– Commission approved data protection clauses

– Legally binding agreements between public authorities

– Commission approved certification

– Binding corporate rules that are enforced across different entities within the same corporate group

The transfer of data is strictly regulated so as to offer each individual in the EU the same protections and rights under EU law regardless of the location of data storage or processing. This has significant implications for organizations in the U.S. that collect, process or store the personal information of EU data subjects. U.S. data protection laws are not considered sufficiently robust by the EU to provide adequate protection, and only organizations certified under the EU-US Privacy Shield agreement will be

compliant with GDPR when it comes into force (exceptions exist in certain circumstances).

GDPR versus Big Data

The GDPR has effects beyond lending, insurance and other firms where sensitive personal data is collected and processed as a matter of course. The rules apply to the human resources record of employees and even the IP addresses of people using online services. The GDPR builds upon data rights that the EU has been pushing for, such as the right of an individual to be forgotten and the right to data portability.

As such, it is expected that the GDPR will lead to data minimization where companies willingly prune down the amount of information they collect to the functional essentials needed to complete a transaction. This could be a reversal of one of the big data trends where companies seek to collect and analyze as much data on their customers as possible in order to gain new insights. This analysis can still take place after appropriate pseudonymization, but other data rights prevent those insights from being used to profile customers in a way that could be discriminatory or put them at a financial disadvantage. As the GDPR is a new regulation, there will no doubt be a period of adjustment where gaps and thorny issues like profiling are addressed.

GDPR KEY CHANGES

An overview of the main changes under GDPR and how they differ from the previous directive

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in today's data-driven world. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR as well as information on the impacts it will have on business can be found below.

Increased Territorial Scope (extraterritorial applicability)

Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in a number of high profile court cases. GDPR makes its applicability very 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 also applies to the processing of personal data of data subjects in the EU by 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 the monitoring of behavior that takes place within the EU. Non-EU businesses processing the data of EU citizens also have to appoint a representative in the EU.

Penalties

Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g.not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors – meaning 'clouds' are not exempt from GDPR enforcement.

Consent

conditions for consent have been strengthened, and companies are no longer able to use long illegible terms and conditions full of legalese. The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Data Subject Rights

Breach Notification Under the GDPR, breach notifications are now mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors are also required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain confirmation from the data controller as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data,

and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent. 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.

Data Portability

GDPR introduces data portability – the right for a data subject to receive the personal data concerning them – which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

Privacy by Design

Privacy by design as a concept has existed for years, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically, '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 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data protection officers

Under GDPR it is not necessary to submit notifications / registrations to each local DPA of data processing activities, nor is it a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there are internal record keeping requirements, as further explained below, and DPO appointment is 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. Importantly, the Data Protection Officer:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on 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 results in a conflict of interest.

THE 8 BASIC DATA PROTECTION RIGHTS OF GDPR FOR CUSTOMERS

The GDPR also defines the rights that individuals have to access and control their data

Under the GDPR, individuals have:

- **The right to access** –this means that individuals have the right to request access to their personal data and to ask how their data is used by the company after it has been gathered. The company must provide a copy of the personal data, free of charge and in electronic format if requested.
- **The right to be forgotten** – if consumers are no longer customers, or if they withdraw their consent from a company to use their personal data, then they have the right to have their data deleted.
- **The right to data portability** – Individuals has a right to transfer their data from one service provider to another. And it must happen in a commonly used and machine readable format.
- **The right to be informed** – this covers any gathering of data by companies, and individuals must be informed before data is gathered. Consumers have to opt in for their data to be gathered, and consent must be freely given rather than implied.
- **The right to have information corrected** – this ensures that individuals can have their data updated if it is out of date or incomplete or incorrect.
- **The right to restrict processing** – Individuals can request that their data is not used for processing. Their record can remain in place, but not be used.

- **The right to object** – this includes the right of individuals to stop the processing of their data for direct marketing. There are no exemptions to this rule, and any processing must stop as soon as the request is received. In addition, this right must be made clear to individuals at the very start of any communication.
- **The right to be notified** – If there has been a data breach which compromises an individual's personal data, the individual has a right to be informed within 72 hours of first having become aware of the breach.

Taken together, these principles and rights make the GDPR the world's most powerful and far-reaching privacy law. Because so much business is now very international, the effect will be that companies outside the EU will conform to GDPR privacy standards in order to access European markets of 500m wealthy consumers.

Following years of data breaches and hacks and scandals about government and corporate intrusion into our private lives, if the GDPR improves the strength of privacy rights across the world, well, this is definitely a good thing.

IMPACTS ON THE FINANCIAL INDUSTRY UNDER GDPR

The recent media reports about an alleged data breach involving social media site Facebook and Cambridge Analytical have added to the ongoing concerns about the safety of personal data from identity theft, cyber-attacks, hacking or unethical usage. The European Union has introduced the new General Data Protection Act (GDPR) to safeguard its citizens by standardising data privacy laws and mechanisms across industries, regardless of the nature or type of operations. It also aims to empower EU citizens by making them aware of the kind of data held by institutions and the rights of the individual to protect their personal information.

1. Consent

The GDPR sets a high standard for consent and defines it as "offering individuals genuine choice and control." Under the GDPR, all of the responsibility for consent is placed upon the company. You will be required to not only ask for an individual's consent before collecting or processing their data, but you must also keep a record of when, how, and what you told each individual about consent. On top of that, companies must also allow individuals to be able to easily withdraw their consent at any time. The UK's Information Commissioner's Office suggests building regular consent reviews into your business processes to ensure continual compliance.

2. Right to Data Erasure

The right to data erasure, also known as the "right to be forgotten", gives an individual the right to have their bank or financial institution completely erase their personal data,

as long as there is not a compelling reason to continue processing. This also applies to data that the financial institution has shared with any third-party organizations. **Companies will need to have robust data inventories and data tracking implemented** in order to effectively and efficiently execute on requests to remove personal data.

3. Consequences of a Breach

The GDPR has very strict requirements if personal data is breached. Under the GDPR, a personal data breach is “any breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.” **An organization has 72 hours to inform relevant supervisors of the breach** once they have been made aware of it. Because it may be impossible to fully investigate the details of a breach within the 72 hour time frame, the GDPR allows for the information to be provided to the necessary parties in phases.

4. Privacy by Design

Privacy by Design is an approach that implements data protection and privacy from the beginning of any business policy, procedure, or project. Willis Towers Watson reports, “‘Privacy by design’ requirements now mean that following a breach, regulators will examine the measures an organisation took to safeguard personal data in order to determine fines.” This means all accountability for compliance and data protection is on the company. It requires that companies show how they are in compliance via organizational and technical controls, not just report that they are in compliance.

For companies who do not meet the requirements or who are found to be noncompliant, the consequences will be severe - with **fines of four percent of your global revenues** or €20 Million, whichever is greater.

5. Vendor Management

Data is at the very core of every financial institution and is constantly being shared through multiple IT applications. It is imperative that each bank and financial firm have a clear process and procedure in place for all external vendors handling their customer data. World Finance states, “The increased trend towards outsourcing development and support functions means that personal client data is often accessed by external vendors, which significantly increases the data’s net exposure. Under GDPR, vendors cannot disassociate themselves from obligations towards data access.

6. Data Protection Officer

Many companies in the finance industry will be required to appoint a Data Protection Officer (DPO) because they “carry out large scale systematic monitoring of individuals”, mostly for the sake of personalized marketing, fraud detection, and customer segmentation. The DPO will be required to monitor the company’s compliance with the GDPR, including managing internal data protection activities, advising on data protection impact assessments, training staff, and conducting internal audits.

IMPACT ON BANKING SECTOR

The following are my views on how implementing GDPR will impact the Banking Sector!

- Data Classification needs to be applied on personal data of customers
- Reporting of data breaches will become mandatory
- A robust Incident Management capability has to be established (Breach Management)
- Secured Communication Channels (Encryption) has to be established
- We need to develop & implement a Data Protection Governance Framework having the relevant policies, processes and roles & responsibilities
- Appointment of Data Protection officer is mandatory (ISO will play this role)
- We may have to revisit the TOR of Information Security Committee to add Data Privacy aspects
- Customer data needs to be deleted based on customer request
- We should get explicit consent from customers on using their personal data for any sort of business purposes
- More rigor has to be applied on KYC Process
- Customers will have the right to transfer the storage of their data based on their preferences
- Customer will have the right to ask their personal data in the format they desire. This will mandate us to have a strong report generation system/capability in place.
- Data Quality has to be given focus and the poor quality data needs to be rectified through periodic reviews.
- Specific clauses need to be introduced into contracts signed with third-party data processing firms used by the bank
- In periodic basis we need to commission privacy impact assessments.
- In periodic basis we need to review and enhance our current IT architecture supporting data storage, transformation and processing of personal data to fulfill GDPR requirements

- We need to develop and implement a Meta Data Management system and establish / expand data lineage to comply with data protection requirements.
- We need to perform a personal data inventory and map all personal data through a glossary.
- IT Systems currently used for data processing have to be designed to ensure best possible data protection from the outset (i.e., compliance with the principles of transparency, of data minimisation of proportionality, etc.).
- An impact analysis will become mandatory if certain categories of personal data (e.g., health, racial and ethnic origin, political opinion, etc.) are processed or processed personal data is used for any kind of profiling.
- Cross border data transfer will be prohibited
- Clear process and procedure to be established in place for managing all external vendors handling our customer data

HOW BANKS SHOULD PREPARE FOR THE GDPR

The financial sector is one of the more highly regulated industries, but many banks have nonetheless been thrown off by the complexity of the EU General Data Protection Regulation (GDPR). The Regulation, which takes effect on 25 May 2018, overhauls the way organisations handle personal data. It includes countless requirements, but this blog outlines three essential steps banks should take as soon as possible.

1. Documenting a lawful basis for processing

Most organisations use consent to process personal data, but the GDPR discourages this practice by toughening the requirements for lawful consent. Organisations should instead use one of the five other lawful bases wherever possible:

- **A contract with the individual**: for example, to supply goods or services they have requested, or to fulfill an obligation under an employee contract.
- **Compliance with a legal obligation**: when processing data for a particular purpose is a legal requirement.
- **Vital interests**: for example, when processing data will protect someone's physical integrity or life (either the data subject's or someone else's).
- **A public task**: for example, to complete official functions or tasks in the public interest. This will typically cover public authorities such as government departments, schools and other educational institutions; hospitals; and the police.
- **Legitimate interests**: when a private-sector organisation has a genuine and legitimate reason (including commercial benefit) to process personal data without consent, provided it is not outweighed by negative effects to the individual's rights and freedoms.

2. Hire a DPO

Most banks will employ someone to oversee the organisation's regulatory compliance – but the GDPR makes this mandatory. The data protection officer (DPO) has many obligations, including:

- Educating employees on the GDPR's compliance requirements;
- Training staff who are involved in data processing;
- Conducting audits; and
- Serving as a point of contact between an organisation and its supervisory authority.

The DPO is required to report to the highest management level (i.e. board level), and the board should provide them with adequate resources to meet their obligations.

3. Prepare for the right to data portability

The right to data portability allows individuals to obtain any information that an organisation holds on them and to reuse it for their own purposes. Individuals are free to either store the data for personal use or transmit it to another data controller.

The data must be received "in a structured, commonly used and machine-readable format".

As law firm Simont Braun explains: "The goal is thus to provide a data subject with the capacity to obtain, reuse and transfer its personal data from one data controller (e.g. Bank A) to another (e.g. a third party payment service provider such as an [account information service provider])."

The right to data portability applies:

- To personal data that an individual has given to a data controller;
- When the processing is carried out by automated means; and
- Where the processing is based on the individual's consent or for the performance or a contract.

The second and third conditions are relatively self-explanatory, but it's less clear exactly what personal data is 'given to' a data controller. The Article 29 Data Protection Working Party clarifies that this refers to information that "relate[s] to the data subject activity or result[s] from the observation of an individual's behavior".

THE IMPACT OF GDPR ON CUSTOMER ENGAGEMENT

The conditions for obtaining consent are stricter under GDPR requirements as the individual must have the right to withdraw consent at any time and there is a presumption that consent will not be valid unless separate consents are obtained for different processing activities.

This means you have to be able to prove that the individual agreed to a certain action, to receive a newsletter for instance. It is not allowed to assume or add a disclaimer, and providing an opt-out option is not enough.

GDPR has changed a lot of things for companies such as the way your sales teams prospector the way that marketing activities are managed. Companies have had to review business processes, applications and forms to be compliant with double opt-in rules and email marketing best practices. In order to sign up for communication, prospects will have to fill out a form or tick a box and then confirm it was their actions in a further email.

KEY CHALLENGES ASSOCIATED WITH THE GDPR

The decision to implement the GDPR has come with criticism. Those opposed to the new regulation say that the position of the DPOs could be an administrative burden for many EU countries. The guidelines were set to include social networks and cloud providers, but did not consider how to deal with employee data. In addition, data cannot be transferred to another country outside the EU, unless it guarantees the same kind of protection. Companies that didn't have this kind of privacy protection may be required to change their business practices. The costs associated with the proposed regulation may also increase (due to the need for more investment) and general education in data protection may also be required. Data protection agencies across the EU will need to agree to a standard level of protection, something that may not be easy as they may disagree in the interpretation of the guidelines.

1. Many new requirements

It’s the EU legislators’ firm intent to increase the accountability of any person processing personal data. How? By imposing responsibilities and requiring to demonstrate compliance therewith at all times. For instance, to encourage transparency, various obligations regulate information, access and communication with the data subject. New and improved rights for the data subject, such as the right to data portability and the right to be forgotten, impact companies because such rights need to be accommodated in their internal processes.

2. Very process-driven

The GDPR sets out specific processes for companies to adopt. It intends to help companies structure and formalize certain subject areas like risk assessment and decision making. By putting these structured processes in place, companies can work more efficiently and achieve compliance with the privacy rules. For instance, a data protection impact assessment (PIA) becomes a mandatory pre-requisite before engaging in any data processing that may result in a high risk to the rights and freedoms of individuals. Also, the privacy-by-design and by-default principles require companies to incorporate privacy into the architecture of their products and services. Furthermore, organizations are expressly encouraged to certify their data processing with a supervisory authority or an approved certification body.

3. Very tangible and visible/verifiable functions and steps need to be realized

It's not only a question of complying with general principles, such as data minimization or accuracy; the GDPR also imposes very concrete measures. For instance, the GDPR imposes an obligation on companies to keep internal records of their data protection activities. Also, data breaches must not only be notified without undue delay but must also be documented, explaining the underlying facts, the effects, and the remedial action taken. And there is more: new roles will be created, such as the Data Protection Officer (DPO). Appointing a DPO can be mandatory, for example for businesses engaging in profiling or tracking online behavior or for biomedical companies that process health data.

4. Increased fines and sanctions

The GDPR could have a huge impact for companies failing to comply. The supervisory authorities can take one or more measures listed in the GDPR, such as (i) issue a warning or impose a temporary or definitive ban on processing personal data, or (ii) impose a fine up to EUR 20,000,000 or 4% of the total worldwide turnover, depending on the circumstances of each individual case, or both.

FUTURE OPPORTUNITIES

Looked at one way, the changes wrought by GDPR aren't too dramatic – it is being described as an evolution, not a revolution. However, over the longer term it may force traditional banks to behave more like challenger banks, replacing their disparate IT systems with more joined-up digital offerings. On top of this, any projects involving personal data will require greater analysis upfront, avoiding unexpected costs and delays further down the line.

Moving beyond compliance, GDPR brings opportunities too. As Cousin explains, there are already a number of firms, including some in the financial sector, using GDPR compliance as a better way of selling their brand.

“GDPR can be an opportunity for developing increased levels of customer engagement and trust,” she says. “It is therefore worth bearing in mind that the GDPR for financial institutions does not only have to be about ever-increasing and stricter regulation.”

Starling Bank, for instance, is working to create a functionality within its app, which would allow customers to access their data at the push of a button.

“In terms of what we’re doing, we’re not just doing it because it’s the law and we want to comply – we think it’s a good thing and are asking what more we can do to make customers’ lives easier,” says Newman. “The question for the industry as a whole is how they keep ahead of technological advances from a data privacy side, while keeping the customer at the heart of it. The sector is really alive to this issue.”

- **Clean house** – the GDPR will require a review of data handling and processing procedures; this presents a great opportunity to review and map your data flows – and restructure them not only for compliance, but also for business efficiency.
- **Clarification** – the GDPR has gone some way to clarifying certain key concepts such as anonymisation and pseudonymization. The GDPR confirms that the principles of data protection do not apply to anonymous information (i.e. information that does not relate to an identified or identifiable natural person or to personal data that does not identify an individual).
- **Pseudonymization** (which means processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information (such as a code or a token)) is encouraged by the GDPR and categorised as an “appropriate safeguard” (along with encryption) for processing personal data.
- **Innovation** – for organisations willing to think outside the box, relatively new concepts such as privacy by design, profiling and data portability present the opportunity not only to innovate, but also to build customer trust and confidence and therefore ultimately drive sales.

FIVE BENEFITS GDPR COMPLIANCE WILL BRING TO YOUR BUSINESS

Most of the media coverage of the EU's General Data Protection Regulation (GDPR) has been focused on the ridiculous multimillion-dollar fines businesses can face if they fail to protect customers' data. Vendors and suppliers play up the same card to boost sales for their products and services. Of course, the price of noncompliance with the GDPR is not something one can afford to shrug off.

However, the problem with concentrating on the punitive side of the GDPR is neglecting new business opportunities. The real driver for adopting new compliance principles should be to make your business more efficient, secure and competitive. Let us take a look at some of the carrots that many may leave out while scaremongering about GDPR sticks.

Benefit One: Enhance Your Cyber security

There is no company in the world that can afford to take the risk of cybersecurity ignorance, given the costs of data breaches and business downtime caused by theft or loss of critical data. It does make sense to take data privacy seriously and the GDPR can help you establish a security-conscious workflow.

The legislation requires organizations to identify their security strategy and adopt adequate administrative and technical measures to protect EU citizens' personal data. It is close to impossible to ensure the integrity and security of specific types of data that travel across the network and leave the rest of the IT environment out of scope. In fact, the regulation encourages you to reevaluate and improve your overall cybersecurity strategy: You will have to establish thorough control over the entire IT infrastructure, build healthier data protection workflows and streamline security monitoring. These activities will help your organization reduce the attack surface, better understand what is going on across your network and decrease the likelihood of having to pay what some organizations think of as a "cyber tax," caused by rising attack numbers and system outbreaks.

Benefit Two: Improve Data Management

To be compliant, you should know precisely what sensitive information you hold on people. Obviously, the first thing you want to do for your GDPR compliance is to audit all the data you have. This will enable you to minimize the data you collect and hold, better organize storages and refine data management processes.

First, you will be able to detect and get rid of redundant, obsolete and trivial (ROT) files that your organization retains, though they don't have business value. By cleaning up the data, you will slash costs on storing and processing this data and probably erase sensitive ROT data, such as former customers' personal information. Such data poses a high and unjustified risk to your organization, so why take responsibility for something that has no value to you.

Second, after you analyze all data you have, you can implement mechanisms for fulfilling another GDPR requirement -- making data globally searchable and indexed. This will help you more easily handle subjects' requests to delete the data if they exercise their right to be forgotten. On the other hand, this requirement will encourage you to reorganize data storages so your staff will be more productive and efficient while working with accurate, easily searchable and accessible data.

Benefit Three: Increase Marketing Return On Investment (ROI)

One of the key principles of the GDPR is that the organization should implement an opt-in policy and have a data subject's consent to process their personal data. Combined with purging irrelevant ROT information stalling your marketing, such as lost leads or unengaged addresses, you will receive a lean fine-tuned database of highly relevant leads and customers that genuinely want to hear from you.

With this information at hand, you will be able to experiment with niche marketing by tailoring your message to the specific needs and habits of a clearly defined audience that has more interest in your brand. Such a granular marketing approach will result in higher click-through, conversion rates and social sharing, and increase your marketing ROI as budgets and efforts will be spent wisely.

Benefit Four: Boost Audience Loyalty And Trust

GDPR compliance can support your business in helping you build more trusting relationships with your customers and the public generally. When gathering consents to use data subjects' data, you will have to explain clearly and concisely how you will be using their personal information. Since consumers are becoming more and more suspicious about how their data is handled, the transparency and responsibility you demonstrate will encourage trust in your brand. Thus, you can use the GDPR to underline that you do care about the privacy of your current and prospective customers and stand head and shoulders above your competitors.

Benefit Five: Become The First To Establish A New Business Culture

There is nothing new about businesses being animal-friendly, eco-friendly, LGBT-friendly, though 10-15 years ago it seemed impossible. Why not become human

privacy-friendly? Organizations should think of their brand as a decent human being that doesn't just consume to sustain itself and grow but also contributes to the community.

The GDPR is a promising first step toward a new business culture that can become a norm just like separating food waste and plastic or recycling old bulbs -- respect and secure the data of all people who entrust their sensitive information to you. By adhering to the GDPR, you will cultivate the values of data security in your employees and nurture social responsibility in business. This way, you will be among the first to introduce a new mindset of respecting customer data privacy.

While no one denies that complying with the GDPR is hard, a wise leader takes this challenge as something more important than just doing the bare minimum to comply. It is time to look forward to the benefits the legislation will bring. They are the benefits that may give your organization the competitive differentiation it needs to succeed and be among the first to implement a new business culture that cherishes human privacy. The GDPR is your opportunity to excel.

The Ten Key Issues Businesses Should Understand While Making Themselves GDPR Compliant

1) **Most stuff is changing, however not the entire thing**—The GDPR makes several necessary changes to EU data protection law, however, it's not an entire departure from existing principles. Several of the ideas that organizations are conversant in can still apply beneath the GDPR.
2) **A DPO should be designated**—Organisations that often and consistently monitor data subjects, or method Sensitive Personal knowledge on an outsized scale, should appoint a Data Protection Officer ("DPO").
3) **The introduction of mandatory Privacy Impact Assessments (PIAs)**—The GDPR makes it mandatory for data controllers to conduct PIAs in the case where privacy breach risks are high. This means before organizations can even begin projects involving personal information, they will have to conduct a privacy risk assessment and work with the DPO to ensure they are in compliance as projects progress
4) **Data subjects rights**—some rights of data subjects are reinforced by the GDPR (e.g., the right to object) and a few new rights are created (e.g., the right to information portability). These rights might build it more durable for organizations to lawfully method personal information
5) **Geographic application**—The GDPR applies to non-EU organizations if they: (i) provide product or services to EU residents; or (ii) monitor the behavior of EU residents. Several organizations that don't seem to be subject to existing EU data protection law are subject to the GDPR, particularly online businesses.

6) **Notifying a data breach within 72 hours**—The GDPR necessitate businesses to report data breaches to the relevant DPA within seventy-two hours of detection. For several organizations, radical changes to internal detailing and investigating structures are going to be required.
7) **Fines**—the penalty structure under GDPR for companies failing to mistakes is a tiered one. More serious infringements will cause a fine of 20 million euros up to four percent of a company's worldwide A lesser fine of up to two percent of worldwide revenue—still huge—are often issued if company records aren't so as or a supervising authority and data subjects aren't notified when a breach has occurred. This makes breach notification oversights a heavy and pricey offense revenue.
8) **Consent—**Consent becomes more difficult for organizations to get and place confidence in. Notably, the GDPR states that consent isn't valid wherever there's a "clear imbalance" between the controller and also the data subject.
9) **Compliance obligations for controllers to be increased**—The GDPR imposes new and hyperbolic compliance obligations on controllers (e.g., implementing acceptable policies, keeping records of process activities, privacy on purpose and by default, etc.
10) **Direct compliance obligations for processors**—Processors have direct legal compliance obligations under the GDPR and DPAs will take social control action against processors, and DPAs can take enforcement control actions against processors.

UNEXPECTED CONSEQUENCES OF GDPR

Fifteen members of Forbes Technology Council discuss some of the more unexpected consequences of the new GDPR regulation. Here's what they had to say:

1. Restriction of Privacy and Innovation

GDPR is the latest version of Y2K compliance -- long on speculation and fear, short on reality. In my opinion, regional enforcement of global technology is impossibility and will restrict -- not enhance -- privacy, freedom and innovation. The result will be regions of non-compliance (GDPR havens), enormous expense and uncertainty. - Wayne Lonstein, VFT Solutions

2. Road blocks For Block chain Data Storage

GDPR could impact the decisions and data sets being stored and collected in emerging private and public blockchains. This may create roadblocks for companies looking to embrace blockchain to store any data that may fall under GDPR. - Aaron Vick, Cicayda

3. Opt-In Fatigue

One of the most unexpected consequences of GDPR is the wave of new regulations in jurisdictions outside of Europe, including California, New York and perhaps soon in Asia. Another unintended impact is "check the box" fatigue where opt-in consent language is presented so frequently on websites and apps that consumers don’t read the consents and just check the box, waiving their privacy rights. - Silvio Tavares, CardLinx Association

4. Poor Customer Service

One GDPR byproduct distortion or unintended consequence is excessive regulation leading to poor customer service. The pendulum has swung too far and will be moderated by citizen feedback. - Jeff Bell, Legal Shield

5. Small Businesses Getting Hurt

The companies that are best prepared for GDPR are the big ones: Facebook, Google, Amazon -- those that have the money to pour into their tech and legal teams for ultimate compliance. The small and medium-sized businesses, however, may be less prepared, making them more vulnerable to potential fines and penalties. - Thomas Griffin, OptinMonster

6. The Slow Death of Free Services

If a service is free, then your data is the product. We all love using Facebook, YouTube and the many other social media platforms. However, we fail to realize how these businesses operate. If regulations strangle business, then the alternative is a paid model. Just look at YouTube and how it's struggling with its paid subscriptions. - Daniel Hindi, Build Fire

7. Talk About Similar Regulation In The U.S.

The most unintended consequence has been the multitudes of discussions about a similar impending regulation in the U.S. In fact, reading between the lines of Facebook's testimony to Congress, it is clear to me that tech leaders realize more care ought to be given to sensitive data, and users should have more rights. They are preparing for coming regulation stateside. - Michael Roytman, Kenna Security

8. Photography Being Part of GDPR

Unexpectedly, photography at work and school is also a part of GDPR. Even if you have asked for consent of employees, parents and students in advance, every depicted person now has a right to ask for photo removal. Companies have to make sure all copies of personal information can be accessed at a moment’s notice, with ongoing assessment and auditable accountability across all systems. - Michael Fimin, Netwrix Corporation

9. C-Suite Becoming Responsible For Data Security

GDPR marks the first time that multiple key departments must be in sync to achieve effective management, especially in light of Gartner’s Integrated Risk Management spectrum, which defines three risk types: strategic, operational and IT. Historically, IT has been responsible for data security and network protection, but GDPR’s requirements make this a C-suite affair. This is a whole new ballgame that many didn’t see coming. - Thomas Sehested, GAN Integrity

10. Restricted Technology Access for EU Citizens

For example, most apps in Apple and Android app stores collect some kind of personal information, and most of these developers are too small to manage these regulations. The unintended consequence being that they will not make these apps available to European residents. Look for GDPR to impact product availability in the EU. - Brent Chapman,RoundPoint Mortgage Servicing Corporation

11. Reduced Ability To Track Cybercrime

An unexpected consequence of the GDPR regulation involves the reduced ability to track and detect cybercriminals. Web domain registration details such as name, address and contacts of domain owners have been crucial in linking malicious sites to hackers. Unfortunately, this outcome was never foreseen since the regulation focused on protecting the consumer data without explaining how malicious users and activities would be addressed. - Rohan Pinto, 1Kosmos BlockID

12. More Meaningful Customer Engagement

Companies with insincere marketing techniques have encountered problems with GDPR. However, the overall effect on the industry is positive, as companies are now forced to have meaningful interactions with their customers. Really engaged customers are far more valuable than uninterested ones. If someone has accepted your services they will interact more, and your marketing efforts will become more effective. - Scott Arpajian, Softonic.com

13. Country Legislation At Odds With GDPR

One consequence we've seen is that country legislation can sometimes contradict GDPR requirements. For example, in transactional solutions, legislation in some countries requires traceability for actions completed by single users. However, GDPR instructs companies to erase all data pertaining to individual actions, meaning that this individual traceability is lost and the ability to audit enterprise workflow activities becomes impossible. - Claus Jepsen, Unit4

14. U.S. Websites Denying Access To EU Visitors

When GDPR came into force, one of the immediate results was an increase in the number of U.S. websites denying or restricting access to EU visitors. We've had two years to prepare ourselves for GDPR, but many weren't truly prepared. It's understandable that some companies might choose the seemingly easier path, but this approach isn't sustainable, at least not in tech or sales. - Timo Rein, PipeDrive.com

15. Increased Value of First-Party Data

As GDPR compliance has taken a hold not only across the EU but across the globe, the value of first-party data has grown exponentially, while third-party data becomes a commodity. First-party data is not only being leveraged to drive personalized experiences, but we're seeing consumers now expect hyper-personalized brand interactions in exchange for the detailed information they provide brands. - Nitay Joffe, ActionIQ

THE POSITIVE AND NEGATIVE IMPLICATIONS OF GDPR

In this article, we are going to discuss the positive and negative and implications of the new GDPR legislation.

The Positive Implications of GDPR

Improved Cybersecurity

Organisations have been in a continuous battle for almost as long as the internet has existed. Security upgrades in networks, servers and infrastructures have been a primary source of cyber protection along with other policy and security changes until recently. The passing of GDPR has directly impacted data privacy and security standards while also indirectly encouraging organisations to develop and improve their cybersecurity measures, limiting the risks of any potential data breach.

Standardization of Data Protection

As mentioned in the second paragraph, GDPR compliance is assessed by Data Protection Agencies from each nation. Although these compliance audits are carried out by independent agencies, the EU-wide standardisation of the regulatory environment ensure once an organisation is GDPR compliant, they are free to operate throughout all European countries without being required to deal with each nation’s individual data protection legislation.

Brand Safety

As some internationally recognised organisations have experienced, data breaches have a monumentally devastating impact on the reputation of an organisation. Users and customers value their privacy and their confidence can be irrevocably damaged if a breach of data does occur and their information is made available unknowingly.

On the opposite end of this spectrum, lies a customer that is more than willing to share their private information as they believe their data is being stored and used in line with GDPR. If an organisation can become a trusted holder of information, their odds in creating a long-lasting and loyal relationship with a customer will improve significantly.

Loyal Customer Following

One of the primary reasons for the formation of GDPR was to allow users to spend more time on the sites they enjoy without being overwhelmed with advertisements from either unsolicited senders or relatively unknown organisations that were subscribed to in the past.

Users and customers are far more likely to accept the mandatory opt-in from organisations and businesses they are interested in. In the near future, a user that subscribes to an organisation will be one that has qualified their interest with subscriptions becoming a sign on loyalty or interest.

The Negative Implications of GDPR

Non-Compliance Penalties

The cost of non-compliance is certainly one that has encouraged organisations to consider their data protection responsibilities inside the EU. With a potential fine of €20m or 4% of Global Annual Turnover the cost of non-compliance, the results of an audit can present a frightening realization of business closure if an organisation fails to protect their customer data.

The Cost of Compliance

When the news first broke that GDPR would be implemented in 2018, most organisations reacted by instating a Data Protection Officer to take responsibility for ensuring internal policies were updated and any required processes were implemented.

Depending on the quantity of EU Citizen data being processed by an organisation, the cost of achieving compliance can vary from hundreds of euro to tens of thousands.

Although GDPR certainly holds some very strong positive implications for both businesses and users, the cost of this can accumulate rather quickly with unforeseen salaries being added to the payroll.

Overregulation

New legislation is also accompanied by the possibility of overregulation. Adding a double opt-in inside a form presents the modern customer with a never-ending message of consent.

The new consent form allows customers to control if and how they are contacted by an organisation, empowering them with the full control of who and how they share their data.

The continuous presence of opting-in may discourage some customers from registering as they delay the requirement of opting-in until they are absolutely certain of their interest.

The Aftermath of Implementation

On the 25th May 2018, after so much planning and discussion, we finally saw GDPR etched into legislation. Overall, the GDPR message is very much in favour of the customer. The new regulations that have been implemented allow users to discover who has their data, why they have it, where it's stored and who is accessing it.

While assessing the positive and negative aspects of GDPR, we feel it’s clear that the pros certainly outweigh the cons. In the coming months and years we will find a digital world that is more unique and cleaner, free from unsolicited mail.

FREQUENTLY ASKED QUESTIONS

What does GDPR stand for?

General data protection regulation.

How did it come about?

In January 2012, the European Commission set out plans for data protection reform across the European Union in order to make Europe 'fit for the digital age'. Almost four years later, agreement was reached on what that involved and how it will be enforced.

One of the key components of the reforms is the introduction of the General Data Protection Regulation (GDPR). This new EU framework applies to organisations in all member-states and has implications for businesses and individuals across Europe, and beyond.

"The digital future of Europe can only be built on trust. With solid common standards for data protection, people can be sure they are in control of their personal information," said Andrus Ansip, vice-president for the Digital Single Market, speaking when the reforms were agreed in December 2015.

What is GDPR?

At its core, GDPR is a new set of rules designed to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy.

What is GDPR compliance?

Data breaches inevitably happen. Information gets lost, stolen or otherwise released into the hands of people who were never intended to see it -- and those people often have malicious intent.

Under the terms of GDPR, not only will organisations have to ensure that personal data is gathered legally and under strict conditions, but those who collect and manage it will be obliged to protect it from misuse and exploitation, as well as to respect the rights of data owners - or face penalties for not doing so.

Who does GDPR apply to?

GDPR applies to any organisation operating within the EU, as well as any organisations outside of the EU which offer goods or services to customers or businesses in the EU. That ultimately means that almost every major corporation in the world will need to be ready when GDPR comes into effect, and must start working on their GDPR compliance strategy.

Why does the GDPR matter?

Any enterprise that collects data from customers is potentially subject to the provisions of the GDPR, and therefore is also subject to the penalties associated with non-compliance. The penalties for non-compliance can be steep, so every enterprise should know and incorporate strict compliance with the GDPR into their business practices and procedures before enforcement becomes active.

Who does the GDPR affect?

Collecting and accepting personal information from any citizen of the EU will invoke the GDPR, regardless of your enterprise's country of origin. For all intents and purposes, if your enterprise has a presence on the internet in the form of a website and if your enterprise collects personal data from customers regardless of where those customers are located, it is subject to the provisions of the GDPR. As a hedge against liability, this essentially means the GDPR applies to every public-facing enterprise.

When will the GDPR take effect?

Technically speaking, the GDPR has been ratified and is currently in effect; however, the EU granted a two-year grace period before beginning enforcement of the provisions in the law. Enforcement goes into effect May 25, 2018..

What has GDPR changed since it was introduced?

As of August, those issues with US publishers still haven't been resolved, with the likes of Tronc still displaying the same apology to users in Europe.

Publishers aren't the only organisations which are having to come to terms with the new reality as some of the largest technology companies including Facebook say they've started to feel the bite of GDPR. The social network has blamed GDPR for a decline of about a million monthly users during the second quarter of the year, as well as a dip in advertising revenue growth within Europe.

Organisations of all sizes have found themselves it to some extent, by users who didn't provide consent for their data to be used when offered the chance to opt in.

Analysts at Forrester say many companies have reported a decrease of between 25 percent and 40 percent of their addressable market for emails and other forms of contact.

As a result, many companies find themselves having to think about new methods of attracting consumers and generating revenue. Analyst Gartner has suggested that some companies may have to rethink their data center strategy as a result of legislation such as GDPR.

What is personal data under the GDPR?

The types of data considered personal under the existing legislation include name, address, and photos. GDPR extends the definition of personal data so that something like an IP address can be personal data. It also includes sensitive personal data such as genetic data, and biometric data which could be processed to uniquely identify an individual.

How does Brexit impact on GDPR?

The UK is set to leave the EU on 29 March 2019, a little over ten months after GDPR comes into force. The UK government has said this won't impact on GDPR being enforced in the country, and that GDPR will work for the benefit of the UK despite the country ceasing to be an EU member. So Brexit is unlikely to have any impact on an organisation's GDPR compliance requirements

What is a GDPR breach notification?

Once GDPR comes into force, it'll introduce a duty for all organisations to report certain types of data breaches which involve unauthorised access to or loss of personal data to

the relevant supervisory authority. In some cases, organisations must also inform individuals affected by the breach.

Organisations will be obliged to report any breaches which are likely to result in a risk to the rights and freedoms of individuals and lead to discrimination, damage to reputation, financial loss, loss of confidentiality, or any other economic or social disadvantage.

If customer data is breached by hackers, the organisation will be obliged to disclose this.

In other words, if the name, address, data of birth, health records, bank details, or any private or personal data about customers is breached, the organisation is obliged to tell those affected as well as the relevant regulatory body so everything possible can be done to restrict the damage.

This will need to be done via a breach notification, which must be delivered directly to the victims. This information may not be communicated only in a press release, on social media, or on company website. It must be a one-to-one correspondence with those affected.

Under GDPR, when does an organisation need to make a notification about a breach?

The breach must be reported to the relevant supervisory body within 72 hours of the organisation first becoming aware of it. Meanwhile, if the breach is serious enough to mean customers or the public must be notified, GDPR legislation says customers must be made responsible without 'undue delay.'

What are the GDPR fines and penalties for non-compliance?

Failure to comply with GDPR can result in a fine ranging from 10 million euros to four per cent of the company's annual global turnover, a figure which for some could mean billions.

Fines will depend on the severity of the breach and on whether the company is deemed to have taken compliance and regulations around security in a serious enough manner.

The maximum fine of 20 million euros or four percent of worldwide turnover -- whichever is greater -- is for infringements of the rights of the data subjects, unauthorised international transfer of personal data, and failure to put procedures in place for or ignoring subject access requests for their data.

A lower fine of 10 million euros or two percent of worldwide turnover will be applied to companies which mishandle data in other ways. They include, but aren't limited to,

failure to report a data breach, failure to build in privacy by design and ensure data protection is applied in the first stage of a project and be compliant by appointing a data protection officer -- should the organisation be one of those required to by GDPR.

When do we need to appoint a Data Protection Officer?

Under the terms of GDPR, an organisation must appoint a Data Protection Officer (DPO) if it carries out large-scale processing of special categories of data, carries out large scale monitoring of individuals such as behavior tracking or is a public authority.

In the case of public authorities, a single DPO can be appointed across a group of organisations. While it isn't mandatory for organisations outside of those above to appoint a DPO, all organisations will need to ensure they have

Failure to appoint a data protection officer, if required to so by GDPR, could count as non-compliance and result in a fine.

What does GDPR compliance look like?

There's no 'one size fits all' approach to preparing for GDPR. Rather, each business will need to examine what exactly needs to be achieved to comply and who is the data controller who has taken responsibility for ensuring it happens.

"You are expected to put into place comprehensive but proportionate governance measures," says the UK's ICO. "Ultimately, these measures should minimize the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place."

That could be the responsibility of an individual in a small business, or even a whole department in a multinational corporation. Either way, budget, systems and personnel will all need to be considered to make it work.

Under the GDPR provisions that promote accountability and governance, companies need to implement appropriate technical and organizational measures. These could include data protection provisions (staff training, internal audits of processing activities, and reviews of HR policies), as well as keeping documentation on processing activities. Other tactics that organisations can look at include data minimisation and pseudonymisation, or allowing individuals to monitor processing, the ICO said.

What will the impact be on firms?

Big organizations have had two years to get ready for GDPR.

The big technology firms that have huge user bases and handle massive amounts of data have spoken about what they are doing. Facebook recently released some new privacy tools that will help it comply with GDPR. Other big technology companies have also released their plans.

"In terms of ad revenue, we see less of an impact, but have heard additional concern around products like custom audiences which all platforms are using. Our checks suggest that most companies using cookies and tags for digital marketing should be relatively unchanged as most
publishers have been using GDPR compliant notifications for months ahead of the May mandate."

Does GDPR Apply to US Citizens Living in an EU Country?

GDPR is not concerned with whether or not an individual is an EU citizen. Anyone located in an EU country is protected by GDPR. If an American travelled to Germany, walked into a store, made a purchase and was required to provide their name and address for an invoice, their personal information would need to be protected in line with GDPR requirements and they be given the same rights and freedoms under GDPR as an EU citizen.

How Does This Affect the US?

When it comes to US businesses, the GDPR requirements will force them to change the way they process, store, and protect customers' personal data. Companies must provide a "reasonable" level of data protection and privacy to its customers, ensuring its storage only upon the individual consent by those customers and no longer than absolutely necessary for which the data is processed. However, the regulation doesn't define what "reasonable" means in terms of ensuring compliance, so this could present future complications when incidents occur and whether or not an organization took *enough* steps to ensure minimal damage.

Upon request, companies must erase personal data—unlike the Cambridge Analytical and Facebook data breach that is still unfolding. The right to be forgotten is a powerful right and a right we as citizens are all entitled to. However, GDPR doesn't supersede any current legal requirement where an organization is required to maintain certain data, like HIPAA requirements.

How Does This Affect Social Media Companies?

Your mind probably just jumped to Facebook and how this will affect social media networks. As we've seen since Mark Zuckerberg's congressional hearing on Capitol Hill

two months ago, many social media companies and online networks have already updated their privacy policies and terms of service in anticipation of today's deadline.

Facebook's response is going to be closely scrutinized by European regulators in wake of the Cambridge analytical breach as well as lingering concerns over the company's data collection. Same with Twitter, yet no major scandal has put them in the public spotlight.

- Accountable EU Representative: If you think social media platforms are exempt from this regulation, you're thinking is also outdated. GDPR requires that social media companies have a designated EU representative that can be held accountable for the GDPR compliance of the organization within Europe.
- Clear Privacy Notice: After hearing Zuckerberg's testimony, it's clear that users need to be presented with a simple and clear privacy notice that they can actually understand—not something that looks like a bulk collection of Harry Potter books bound together.
- The Right To Be Forgotten: It will be interesting to see how these companies will deal with user requests for deletion of certain personal data. It is no longer safe for a company to assume that their customers or users are content with their personal data being held—seeing as most of the have no idea it's held until something unfortunately happens.

What Happens If You Fail To Comply With GDPR?

Failing to adhere to the GDPR has steep penalties of up to €20 million, or 4% of global annual turnover, whichever is higher. Reports estimate that about half of U.S. companies that should be compliant on GDPR requirements by today, won't be. There's more to it than all those emails coming to your inbox about updated privacy terms.

According to a December 2016 PwC survey, 68 percent of U.S. based companies expect to have spent $1-$10 million to meet these GDPR requirements.

But, some websites in the U.S. have services entirely rather than adhere to the new regulations, going completely dark. Dozens of American newspapers are currently blocked in Europe and web services like Instapaper have suspended operations in the European Union for the foreseeable future.

Facebook and Google Already Hit With $8.8 Billion Lawsuit for GDPR Violations

The GDPR is no joke and nothing to mess around with. Not even one day has passed, and

Today is a big day for every business and organization in the world. Let’s hope that the companies we are loyal to, are loyal to us.

Does it Matter Where a Business Is Located?

GDPR applies to individuals and gives them certain rights and freedoms. GDPR places certain restrictions on what businesses can do with the personal data of individuals residing in the EU. It does not matter where the business is located and whether or not a business has a base in an EU country. GDPR rules apply if the business collects or processes the personal data of an individual residing in the EU.

Unfortunately, there is no law that protects the privacy of all individuals in the United States, only specific groups of individuals. The Health Insurance Portability and Accountability Act (HIPAA) requires safeguards to be implemented to protect the privacy of patients and health plan members, but only in relation to protected health information (PHI) and only if PHI is collected, stored, used, or transmitted by a HIPAA-covered entity.

For HIPAA-covered entities, compliance with GDPR will be more straightforward if they apply the same requirements for safeguarding PHI to all individuals and all personal data. Taking a more holistic approach to data protection makes compliance with GDPR easier.

If that approach is taken, then it is likely that EU citizens residing in the US will be given the same protections as those living in an EU country.

Is this privacy email really from an actual company? Could it be a scam?

Organisations of all sizes in all sectors are sending customers emails, asking them to opt-in in order to keep receiving messages and other marketing material. For the most part, if the customer does want to remain on the list, they just need to click the part of the email that tells the company they wish to remain in touch.

However, with so many organisations sending out emails on GDPR, criminals and scammers have taken it up as a prime opportunity to send out phishing emails in order to catch people unaware - especially given how people might be receiving more emails from organisations than usual right now.

Researchers at Red scan uncovered one of these schemes, which sees criminals posing as Airbnb and claiming that the user won't be able to accept new bookings or send messages to prospective guests until a new privacy policy is accepted. The

attackers specifically mention new EY privacy policy as the reason for the message being sent.

However, those behind this scheme are very much leveraging GDPR in order to steal information, because while the real Airbnb message doesn’t ask for any information, those who receive the fake message are asked for their personal information, including account credentials and payment card information.

It's unlikely to be the only attempt by criminals to piggyback on GDPR for their own gain..

How can I process data under the GDPR?

GDPR states that controllers must make sure it's the case that personal data is processed lawfully, transparently, and for a specific purpose.

That means people must understand why their data is being processed, and how it is being processed, while that processing must abide by GDPR rules.

What do you mean by 'lawfully'?

'Lawfully' has a range of alternative meanings, not all of which need apply. Firstly, it could be lawful if the subject has consented to their data being processed. Alternatively, lawful can mean to comply with a contract or legal obligation; to protect an interest that is "essential for the life of" the subject; if processing the data is in the public interest; or if doing so is in the controller's legitimate interest – such as preventing fraud.

At least one of these justifications must apply in order to process data.

How do I get consent under the GDPR?

Consent must be an active, affirmative action by the data subject, rather than the passive acceptance under some models that allow for pre-ticked boxes or opt-outs.

Controllers must keep a record of how and when an individual gave consent, and that individual may withdraw their consent whenever they want. If your current model for obtaining consent doesn't meet these new rules, you'll have to bring it up to scratch or stop collecting data under that model when the GDPR applies in 2018.

What is personal data?

Personal data can be anything that allows a living person to be directly or indirectly identified. This may be a name, an address, or even an IP address. It includes automated personal data and can also encompass pseudonymise data if a person can be identified from it.

What’s sensitive personal data?

GDPR calls sensitive personal data as being in 'special categories' of information. These include trade union membership, religious beliefs, political opinions, racial information, and sexual orientation.

When can people access the data we store on them?

Aiming to give users and customers more rights and power over their own information, GDPR stipulates that people can lodge requests to access their data from organisations.

Anybody can submit a subject access request (SAR) with data controllers, and if deemed reasonably (certain exemptions apply) the organisation will have a month to fulfill the request in full. A SAR provision already in UK law prior to GDPR, but the new regulation reduced the legal time limit from 40 to 30 days.

GDPR dictates that controllers and processors both must establish clearly how information is collected, what purposes data is used it for, and the ways in which this data is processed. Clear and plain language must also be used consistently across any messaging, restricting the liberty many firms took in sending reams of dense and complex information to consumers in order to obfuscate objectionable data practices.

By submitting a SAR users exercise their right to know what data a company holds on them, and how their data is processed, among a number of other facts.
Users and customers can also ask for data, if it is wrong or incomplete, to be corrected and brought up-to-date any time.

Refusing to comply with SARs constitutes a potential breach, with a number of companies, including Twitter, currently facing a GDPR investigation for failing to provide users with the appropriate information requested.

What's the 'right to be forgotten'?

GDPR makes it clear that people can have their data deleted at any time if it's not relevant anymore - i.e. the company storing it no longer needs it for the purpose they collected it for. If the data was collected under the consent model, a citizen can withdraw this consent whenever they like. They might do so because they object to how an organisation is processing their information, or simply don't want it collected anymore.

The controller is responsible for telling other organisations (for instance, Google) to delete any links to copies of that data, as well as the copies themselves.

What if they want to move their data elsewhere?

Then you have to let them – and swiftly: the legislation means citizens can expect you to honor such a request within four weeks. Controllers must ensure people's data is in an open, common format like CSV, meaning that when it moves to another provider it can still be read.

Is the Investigatory Powers Act compatible with GDPR?

However, what's unclear is whether other new legislation will be deemed compatible with GDPR once the UK leaves the EU. For example, under the UK's Investigatory Powers Act, ISPs are compelled to collect personal web histories and hold them for up to 12 months. The government currently has to rewrite some of these laws after identical powers in old DRIPA legislation were found to be illegal.

But Hancock wrote in October 2017 that "UK national security legislation should not present a significant obstacle to data protection negotiations."

Is this worldwide?

GDPR applies only to the EU, but given the scale of the market, many companies are deciding it's easier – not to mention a public relations win – to apply its terms globally. Apple's privacy tools are worldwide, for instance, as are Facebook's (although the latter won't promise to apply every aspect of GDPR globally, noting that the rules may clash with privacy regulations in other jurisdictions).

REFERENCES

- https://www.cnbc.com/2018/03/30/gdpr-everything-you-need-to-know.html
- https://www.hipaajournal.com/does-gdpr-apply-to-eu-citizens-living-in-the-us/
- https://www.privacytrust.com/gdpr/index.html
- https://www.privacytrust.com/gdpr/data-breach-notification.html
- https://www.privacytrust.com/gdpr/gdpr-consent.html
- https://www.privacytrust.com/gdpr/gdpr-consent-requirements.html
- https://www.privacytrust.com/gdpr/first-steps-towards-gdpr.html
- https://www.privacytrust.com/gdpr/gdpr-enforcement-date.html
- https://www.privacytrust.com/gdpr/privacy-by-design-gdpr.html
- https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
- https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp
- https://eugdpr.org/the-regulation/
- https://medium.com/@adityavats/10-key-issues-of-general-data-protection-regulation-gdpr-d70e3875b59e

ARTICLES

- https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/#60a554ea55e5
- https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection
- https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles
- https://www.hipaajournal.com/what-countries-are-affected-by-the-gdpr/
- https://www.privacytrust.com/gdpr/how-to-make-the-gdpr-a-success.html
- https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/
- https://www.techrepublic.com/article/how-the-gdpr-will-make-consumers-king-of-their-data/
- https://www.techrepublic.com/article/the-eu-general-data-protection-regulation-gdpr-the-smart-persons-guide/
- https://www.itpro.co.uk/it-legislation/27814/what-is-gdpr-everything-you-need-to-know
- https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you
- https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018
- https://www.coredna.com/blogs/general-data-protection-regulation
  https://www.hipaajournal.com/overview-of-the-gdpr/
- https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/
- https://digiday.com/media/impact-gdpr-5-charts/
- https://www.superoffice.com/blog/gdpr/
- https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#2a583a1494ad
- https://www.timedatasecurity.com/blogs/the-positive-and-negative-implications-of-gdpr
- https://www.itproportal.com/features/the-negative-impacts-of-gdpr/
- https://www.hldataprotection.com/2018/05/articles/international-eu-privacy/the-true-global-effect-of-the-gdpr/
- https://www.itgovernance.eu/blog/en/how-banks-should-prepare-for-the-gdpr
- https://www.brickendon.com/articles/top-five-impacts-gdpr-financial-services/
- https://www.financialdirector.co.uk/2018/06/21/gdpr-how-is-it-affecting-banks/
- http://m.bankingexchange.com/news-feed/item/7503-is-your-bank-ready-for-gdpr
- https://www.barclayscorporate.com/insight-and-research/managing-your-business/gdpr.html

- https://www.bankrate.com/uk/current-accounts/gdpr-explained/
- https://securereading.com/how-gdpr-will-impact-banking-sector/
- https://www.logicgate.com/blog/post/gdpr-industry-focus-how-does-the-gdpr-impact-financial-services
- http://www.armstrongint.com/what-the-gdpr-means-for-the-banking-industry/
- https://www.nexmo.com/blog/2017/11/14/gdpr-means-customer-communications/
- https://digitalguardian.com/blog/what-does-gdpr-mean-for-you
- http://theconversation.com/what-does-gdpr-mean-for-me-an-explainer-96630
- https://www.virtual-college.co.uk/news/virtual-college/2018/01/the-differences-between-gdpr-and-data-protection
- https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business/#7a3b3050482f
- https://www.evry.com/en/news/articles/the-gdpr--creating-new-business-opportunities2/
- https://www.information-age.com/gdpr-good-not-bad-opportunities-123466100/
- https://cimt.nl/chances-challenges-gdpr/
- https://www.stibbe.com/en/expertise/practiceareas/data-protection/general-data-protection-regulation/what-are-the-challenges
- https://www.hipaajournal.com/what-countries-are-affected-by-the-gdpr/
- https://www.techrepublic.com/article/how-the-gdpr-will-make-consumers-king-of-their-data/
- https://blog.claimable.com/a-brief-history-of-the-gdpr/

REPORT PREPARED BY SARA ZEB AFRIDI