

Personal Data Protection and GDPR



Index

1. Introduction	6
2. GDPR.....	7
2.1. Principles of GDPR.....	8
2.2. Using, processing, storing and transferring data in EU	9
2.3. Consent regarding data processing.....	11
2.4. Right to access and right to data portability	14
2.5. Data breaches.....	15
2.6. Fines	15
2.7. Preparations for GDPR compliance	16
3. ePrivacy	20
3.1. Key points of the European Commission proposal.....	21
3.2. Stronger privacy rules for electronic communications	22
3.3. Applicable law and cross-border situations	23
3.4. Relationship between GDPR & ePR.....	23
3.5. Benefits for citizens and businesses	24
4. Personal data protection	25
4.1. What regulations complement the European regulations	26
4.1.1. Austria.....	26
4.1.2. Czech Republic.....	26
4.1.3. Portugal	27
4.1.4. Spain	29
5. Non-personal data	34
5.1. Free movement of data within the EU.....	35
5.2. Porting of data.....	36
5.3. Procedure for cooperation between authorities	36



5.4. Data availability for competent authorities	37
5.5. Penalties for breaches	37
6. Systematized content catalogue	38
7. Conclusions.....	39
8. References	40



List of abbreviations

DPA: Data Protection Authority

DPO: Data Protection Officer

DSG: Austrian data protection act Datenschutzgesetz

DSVGO: German Datenschutz-Grundverordnung

EEA: European Economic Area

ePR: ePrivacy Regulation

EU: European Union

GDPR: General Data Protection Regulation



Figures

Figure 1 - GDPR	7
Figure 2 - Principles of GDPR	8
Figure 3 - Processing personal data	9
Figure 4 - Data controller and data processor	10
Figure 5 - Processing personal data	12
Figure 6 - Consent example.....	13
Figure 7 - Rights under GDPR	14
Figure 8 - GDPR compliance.....	16
Figure 9 - ePrivacy rules.....	21
Figure 10 - Privacy protection online	23
Figure 11 - GDPR vs ePR	24
Figure 12 - Benefits for citizens and businesses.....	24
Figure 13 - Non personal data.....	34

Tables

Table 1 - Personal data protection legislation	31
---	-----------



1. Introduction

Nowadays the world depends more and more on data because data can add significantly value to numerous economic agents. In the European Union (EU), there are regulations regarding the personal data: Regulation (EU) 2016/679 (General Data Protection Regulation) and the ePrivacy regulation (ePR) that is a proposal for the Privacy and Electronic Communications Directive 2002 (ePrivacy Directive 2002/58/EC).

The Regulation (EU) 2018/1807 aims to remove obstacles regarding the free movement of non-personal data across EU member states and Information Technology in Europe. Along with the General Data Protection Regulation (GDPR), this regulation ensures a comprehensive and coherent approach to the free movement of all data in Europe. The scope of the ePR is to reinforce trust and security in the digital single market by updating the legal framework on ePrivacy (ePR).

These three regulations apply to each European country even though there are some opening clauses that leave the national legislators some leeway.

In this report you can find the most important information related to these legislation. Additionally, in this document we will discuss how the European legislation about personal data protection has been adapted in Austria, Spain, Portugal and Czech Republic.



2. GDPR

The GDPR (Regulation (EU) 2016/679) is an EU law on data protection and privacy for all individual citizens of the EU and the European Economic Area (EEA). It also addresses the export of personal data outside the geographic areas mentioned above. The GDPR is in force since May 2018 and has three main goals:

- a) **Harmonize data privacy laws** across Europe;
- b) **Protect and empower all EU citizens data privacy**;
- c) **Reshape the way organisations across the region approach data privacy.**

Figure 1 - GDPR



Source: Business2Community (2019)

With the GDPR, Europe is signaling its firm stance on data privacy and security and the GDPR reshapes the way in which companies/organizations manage data. The GDPR is applied to:

- a) A **company or entity which processes personal data as part of the activities of one of its branches established in the EU**, regardless of where the data is processed; or,
- b) A **company or entity established outside the EU that offers goods/services** (paid or free) or that monitorize the behavior of individuals in the EU.

2.1. Principles of GDPR

The GDPR has some general principles regarding the process of personal data. One of these principles requires that data is processed transparently which means that this process must be clear and legitimate. Also, the amount of processed data has to be kept to a minimum, depending on the purpose the data has to be accurate and the storage time has to be limited to a period that is bound to the purpose. Additionally, integrity and confidentiality of the data have to be protected. The main principles of GDPR are present in the next figure.

Figure 2 - Principles of GDPR



Source: I-scoop (2019)

Generally, the main contact point for questions on data protection is the Data Protection Act (DPA) in each EU member state where your company/organization is based. However, if your company/organization processes data in different EU member states or is part of a group of companies established in different EU member states the main contact point can be a DPA in another EU member state.

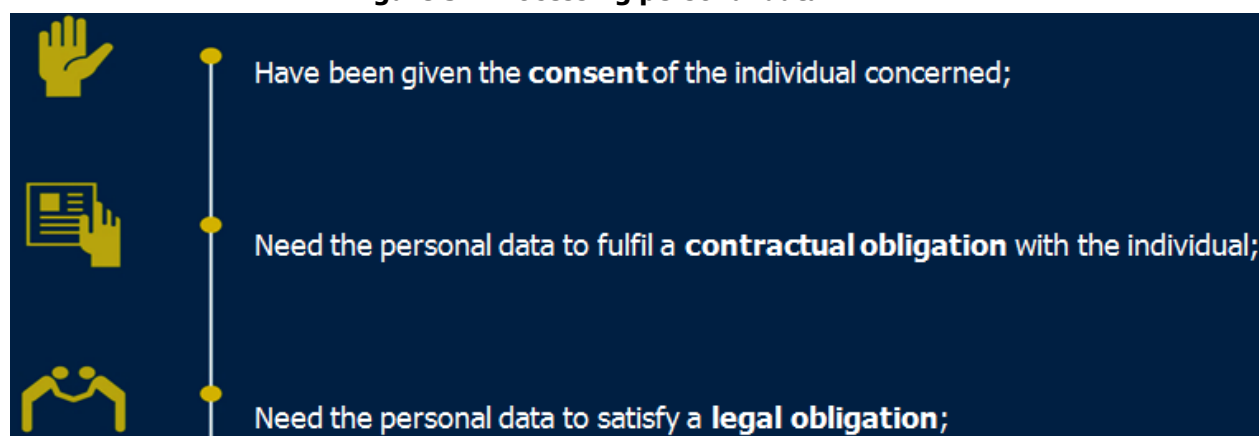
Find your National Data Protection Authority at:




https://edpb.europa.eu/about-edpb/board/members_en

2.2. Using, processing, storing and transferring data in EU

As an individual, company or organisation you have the right to use, collect, store, transfer or manage personal data and to use data centers or cloud services anywhere in EU. The rules for dealing with personal data differ from the rules for the non-personal data. Nevertheless, personal and non-personal data are often collect and stored together and this is known as mixed data. There are some topics that the companies/organisations must fulfil when processing the personal data that are present in the next figure.

Figure 3 - Processing personal data



	• Need the personal data to protect the vital interests of the individual;
	• Process personal data to carry out the tasks in the interest of the public ;
	• Are acting in your company's legitimate interests , as long as the fundamental rights and freedoms of the individual whose data are processed are not seriously impacted.

Source: European Commission (2019)

During processing, personal data can pass through different companies or organisations and within this cycle there are two main profiles that deal with processing personal data: the data controller and the data processor.

Figure 4 - Data controller and data processor



Data controller: decides the purpose and the way in which personal data is



Data processor: holds and processes data on behalf of a data controller

processed

Source: Own elaboration

Companies/organisations that process data are obliged to keep records of processing activities, unless they have less than 250 employees. Also, companies/organisations have to designate a Data Protection Officer (DPO) when one of the following aspects applies:

- When the processing is carried out by a public body (except courts);
- When the core activities of the processor “consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale”;
- When special categories of data or “data relating to criminal convictions and offences” are being processed.

The DPO is someone that may have been designated by the company and is responsible for monitoring how personal data is processed and to inform and advise employees who process personal data about their obligations. The DPO can be a staff member of your organisation or may be contracted externally on the basis of a service contract. The DPO also cooperates with the Data Protection Authority (DPA) serving as a contact point towards the DPA and the citizens.

2.3. Consent regarding data processing

The responsibility to comply with the GDPR depends on companies/organisations that process personal data. Taking into account the nature, scope, context and purposes of processing as well as severity for the rights and freedoms of citizens, the controller shall implement appropriate technical and organisation measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation. Those measures shall be reviewed and updated if necessary. Examples of these measures are pseudonymisation or encryption.

The GDPR applies strict rules for processing data based on consent. The purpose



of these rules is to ensure that the individual understands what he/she is consenting to. This means that consent should be freely given by an affirmative act, such as checking a box online or signing a form. When someone consents the processing of his/hers personal data, you can only process the data for the purposes for which consent was given. It is also important to say that you must clearly provide individuals with information regarding who is processing the personal data about them and the reasons why. For example, the following figure should be included as a minimum:

Figure 5 - Processing personal data



Source: European Commission (2019)

In some situations, the information you provide must also state:

- The contact information of the DPO (if applicable);
- What is the legitimate interest pursued by the company when you rely on this legal ground for processing;
- The measures applied for transferring the data to a country outside the EU;
- How long the data will be stored for;
- The individual's data protection rights;
- How consent can be withdrawn (when consent is the legal ground for processing);
- Whether there is a statutory or contractual obligation to provide the data;

- In the case of automated decision-making, information about the logic, significance and consequences of the decision.

It is important to note that this information should be clear and you must use a simple/plain language.

The conditions for consent have been strengthened and companies/organizations are no longer able to use long illegible terms and conditions full of legal terms and concepts. 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 and language.

The next figure shows an example of what should be done. In next figure you can see that GDPR has changed a lot of things for companies/organizations. Therefore, companies have to review their business processes, applications and forms to be compliant with e-mail marketing for example. 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.

Figure 6 - Consent example

The figure compares two versions of a 'Try SuperOffice CRM for free' form. The left form is labeled 'Not compliant' and the right form is labeled 'GDPR compliant'.

Not compliant form (Left):

- Fields: Your name, Company name, Your email, Your phone.
- Button: Start Free Trial
- Text: By signing up to a free trial of SuperOffice CRM, you agree to our Terms and you have read our privacy policy. You may receive email updates from SuperOffice and you can opt out at any time.

GDPR compliant form (Right):

- Fields: Your name, Company name, Your email, Your phone.
- Buttons: Start Free Trial
- Text: By signing up to a free trial of SuperOffice CRM, you agree to our Terms and privacy policy.
- Text: Yes, please keep me updated on SuperOffice news, events and offers.
- Text: Terms & privacy policy

Source: SuperOffice (2019)

2.4. Right to access and right to data portability

Companies and organisations must ensure that individuals have the right to access their personal data, free of charge. If you receive such a request you have to:

- Tell them if you're processing their personal data;
- Tell them about the processing (the purpose of the processing, categories of personal data concerned, etc);
- Give them a copy of the personal data being processed (in an accessible format).

With the new GDPR, it becomes more important to inform the customer or the person whose data you process about what happens to their data. The rights that you have to be aware of are summed up in the following figure.

Figure 7 - Rights under GDPR



Source: Serveit (2019)

These rights are given to individuals to protect their private lives and control the digital footprints they leave behind when using internet-based applications and services.

These rights are meant to create openness, control and trust between all the parties.

2.5. Data breaches

A data breach is when the personal data is disclosed, either accidentally or unlawfully, to unauthorized recipients is made temporarily unavailable or is altered.

If a data breach does occur and the breach poses a risk to individual rights and freedoms, you should notify your DPA within 72 hours after becoming aware of the breach.

2.6. Fines

Fines are getting bigger and the timelines are getting shorter. Under the GDPR, breach notifications are now mandatory in all members 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 costumers, the controllers without undue delay after first becoming aware of a data breach.

Therefore, the GDPR introduces a tougher enforcement regime and it exposes entities to increased financial liability. Several high level cases are ongoing and could cause fines up to 4% of the annual of a business if there is a serious infringement. The maximum penalty is 20 million euros or 4% of global revenue, whichever is higher. Data protection authorities can also issue sanctions such as bans on data processing or public reprimands.

Under GDPR, fines are administered by the data protection regulator in each EU country. The final amount of the fines will be assessed and in what amount: gravity and nature; intention; mitigation; precautionary measures; history; cooperation; data category; notification; certification; aggravating/mitigating factors. If regulators determine an organization has multiple GDPR violations, it will only be penalized for the most severe one, provided all the infringements are part of the same processing operation.



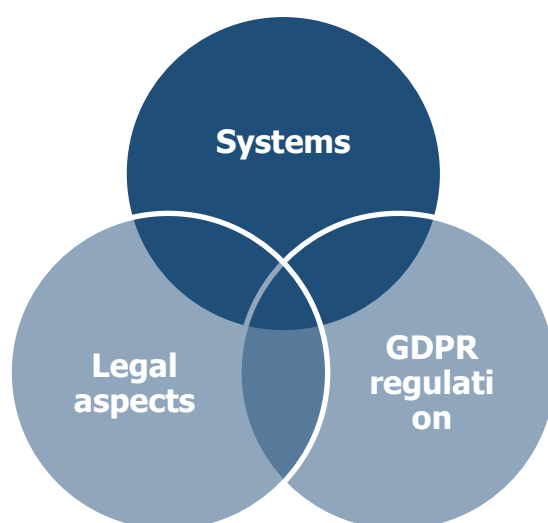
2.7. Preparations for GDPR compliance

The application of GDPR imposes strict requirements on the way companies/organizations collect, store and manage personal data. Having this in mind, GDPR provides citizens of the EU greater control over their personal data and assures that their information is being securely protected across Europe, regardless of whether data processing takes place in the EU or not.

GDPR encompasses three main areas that every business needs to consider (see figure 5):

1. The **GDPR** regulation itself;
2. The **systems** you use to store all your customer data;
3. The **legal aspects** of the regulation and how it will affect the way you handle personal data.

Figure 8 - GDPR compliance



Source: Own elaboration

In addition, a key component of the GDPR legislation is privacy by design. Privacy by design requires that all departments in a company/organization look closely at their data and how they handle it. There are many topics a company has to do in order to be compliant with GDPR. Please find some steps that can help to get this process

started.

- 1. Map your company's data:** Map where all of the personal data in your entire business comes from and document what you do with the data. Identify where the data resides, who can access it and if there are the risks associated to the data that you have.
- 2. Determine what data you need to keep:** GDPR encourages a more disciplined treatment of personal data. Because of that, it is crucial to keep only the information than necessary and remove any data that you aren't using. If your company/organization has collected a lot of data without any real benefit/use, is the time to consider which data is important to your company/organization. In the cleaning process you can follow the questions above:
 - Why exactly are we archiving this data instead of just erasing it?
 - Why are we saving all this data?
 - What are we trying to achieve by collecting all these categories of personal information?
 - Is the financial gain of deleting this information greater than encrypting it?
- 3. Put security measures in place:** develop and implement safeguards throughout your infrastructure to help contain any data breaches. This means putting measures in place against data breaches and taking quick action to notify individuals and authorities in the event a breach does occur.
- 4. Review your documentation:** under GDPR, individuals have to explicitly consent the acquisition and processing of their data. Pre-checked boxes and implied consent will not be acceptable anymore.

2.8. Awareness of the GDPR - one year after the implementation

After one year of implementation the GDPR, the most important and significant change in the data protection legal framework, the European citizens are becoming more aware of the rights and duties that the application of the personal data protection legislation.

According to the results published in June 2019 of the report "General Data Protection Regulation" carried out by the European Commission showed that the majority (more than two thirds) of the Europeans have heard of the GDPR and they also have heard about the rights guaranteed by GDPR, with the exception of the right to have a say when decisions are automated (41%). Additionally, the countries that are know more of GDPR are: Sweden (90%), Netherlands (87%) and Poland (86%). In addition, respondents aged 25-54 (75%) are the most likely to have heard of GDPR, respondents aged 15-54 are more likely than those aged 55 or older to be aware of their personal data rights and men are more likely to be aware of each of these rights compared to women. The longer a respondent remained in education, the more likely they are to be aware of this legislation.

Additionally, Ireland, Slovakia and Poland have some of the highest proportions of respondents who have heard of GDPR and know what it is and also the highest proportions of respondents who have heard of all the rights asked about in the survey that was carried out.

Concerning the awareness of national public authorities in charge of data protection, the majority (6 in 10) say they have heard about the existence of public authority in their country responsible for protecting their rights regarding their personal data.

Since 2018, the national data protection authorities are in charge of enforcing the new rules and are better coordinating their actions. Nevertheless, there is still some work to do when it comes to the compliance issues because this is a dynamic process.

According to the Deloitte Legal report "The GDPR: Six months after



implementation: Practitioner perspectives” there are still some work to do concerning the implementation of GDPR. The most important conclusions of these report suggested that is important to:

- The first thing to do when it comes to compliance with the GDPR is to get to know the details about the processing of personal data because there is still a lack of awareness of basic rules;
- Improve the transparency about the processing of personal data to data subjects as required under the GDPR;
- Improve the guidance, recommendations or official positions from the data protection supervisory of the country;
- Conducting staff awareness trainings and engage all the people with the most relevant GDPR requirements because everyone need to understand how to apply and implement in their everyday work;
- The introduction of security measures that go beyond the required minimum standards (for example the encryption of all the documents attached to e-mail);
- Create a non-commercial platform to share specialized legal knowledge, good practices and practical and creative solutions among personal data protection specialists;
- Guidelines for small and medium sized businesses in order to help them to apply new legal regulation on personal data protection in practice;
- Creation of several templates to deal with several issues related to the GDPR (collect, implement and transfer personal data protection and request permission to transfer personal data;
- Develop of some initiatives target at schools and training materials since early stages.



3. ePrivacy

The Digital Single Market Strategy aims to increase trust and the security of digital services. The reform of the data protection framework, in particular the adoption of the GDPR, was a key action to this. The Digital Single Market Strategy also announced the review of Directive 2002/58/EC (the ePrivacy Directive) in order to provide a high level of privacy protection for users of electronic communications services.

The ePrivacy Directive sets some rules guaranteeing the protection of privacy in the electronic communications sector. Electronic communications includes e-mail; applications; telephone; instant messaging; spam; direct marketing; telecommunication firms; mobile app developers; online advertising networks among many others. This directive also provides protection for users and subscribers of electronic communications services against unsolicited communications.

The ePrivacy Directive requires providers of electronic communications services such as internet access and fixed and mobile telephone to:

- a) Take appropriate measures safeguarding the security of electronic communications services;
- b) Ensure confidentiality of communications and related traffic data in public networks.

The **three main goals of ePrivacy Directive** are as follows:

- Ensure an equivalent level of protection across the EU of the fundamental right to privacy and confidentiality with respect to the processing of personal data in the electronic communications sector. This protection is also granted to subscribers who are legal entities;
- Ensure an equivalent level of protection with respect to the processing of personal data in the electronic communications sector to protect the fundamental right to data protection;



- Ensure free movement of personal data processed in the electronic communications sector and the free movement of electronic communications terminal equipment and services in the EU.

The ePR will replace the EU existing ePrivacy Directive and Electronic Communications Directive 2002. This regulation is important because it means that it will be a legal act and enforceable in its entirety across all member states like GDPR. In addition, this proposal must ensure consistency with the GDPR.

While the GDPR ensures the protection of personal data, the ePR aims to ensure the confidentiality of communications which may also contain non-personal data and data related to a legal person.

The ePR was due to come into force on 25th May 2018 alongside with the GDPR, however, continued deliberation and lobbying of some have delayed the application of this regulation.

3.1. Key points of the European Commission proposal

The proposal for a regulation on high level of privacy rules for all electronic communications includes:

Figure 9 - ePrivacy rules

Communications content and metadata: privacy is guaranteed for communications content and metadata for example, time of a call and location. Metadata have a high privacy component and is to be anonymised or deleted if users did not give their consent, unless the data is needed for billing.

New players: Privacy rules will in the future also apply to new players providing electronic communications services such as WhatsApp, Facebook Messenger and Skype. This will ensure that these services guarantee the same level of confidentiality of communications as traditional telecoms operators.

Stronger rules: All people and businesses in the EU will enjoy the same level of protection of their electronic communications through this directly applicable regulation. Businesses will also benefit from one single set of rules across the EU.

New business opportunities: once consent is given for communications data - content and/or metadata - to be processed, traditional telecommunications operators will have more opportunities to provide additional services and to develop their businesses.

Simpler rules on cookies: the cookie provision, which has resulted in an overload of consent requests for internet users, will be streamlined. The new rule will be more user-friendly as browser setting and other identifiers. The proposal also clarifies that no consent is needed for non-privacy intrusive cookies improving internet experience or cookies used by a website to count the number of visitors.

Protection against spam: this proposal bans unsolicited electronic communications by emails, SMS and automated calling machines. Depending on national law people will either be protected by default or be able to use a do-not-call list to not receive marketing phone calls. Marketing callers will need to display their phone number or use a special pre-fix that indicates a marketing call.

More effective enforcement: the enforcement of the confidentiality rules in the regulation will be the responsibility of data protection authorities, already in charge of the rules under the GDPR.

Source: European Commission (2019)

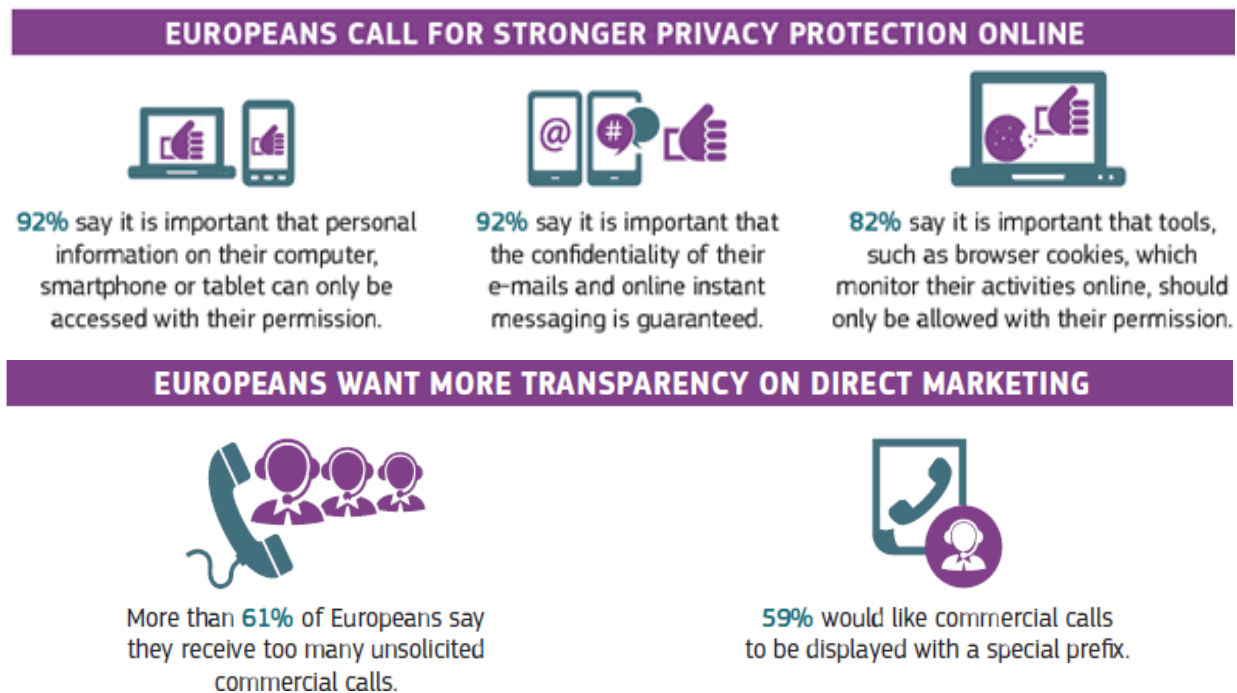
3.2. Stronger privacy rules for electronic communications

As we seen before, more and more Europeans use online communication services and with the ePR Europeans electronic communications are confidential regardless of the technology used, the proposed rules will also apply to internet-based voice and internet-messaging services.

In the next figure, we can observe that Europeans need stronger privacy protection online especially on their mobile devices (computer, smartphone or tablet).

In addition, Europeans want more transparency on direct marketing. Because of that, with this regulation people will have to agree before marketing messages are addressed to them by automated calling machines, SMS or e-mail for example. They will also have to agree to receive marketing calls, unless national law gives them the right to object to the reception of such calls. Additionally, marketing callers will need to display their phone number or use a special pre-fix that indicates a marketing call.

Figure 10 - Privacy protection online



Source: European Commission (2017)









3.3. Applicable law and cross-border situations

The ePrivacy Directive does not contain an explicit provision with regard to the applicable national law. This may create legal uncertainty as to which law should apply in a cross-border context. The unclear situation derives from the lacking of a specific applicable law rule, which hinders an effective application of the rules in a cross-border situation.

3.4. Relationship between GDPR & ePR

There are few differences and similarities regarding the GDPR and the ePR. While the ePR protects the confidentiality of electronic communications the GDPR protects personal data. This means that the ePR complements GDPR in the electronic communications sector. In the next figure we have a comparison between GDPR and the ePR.

Figure 11 - GDPR vs ePR

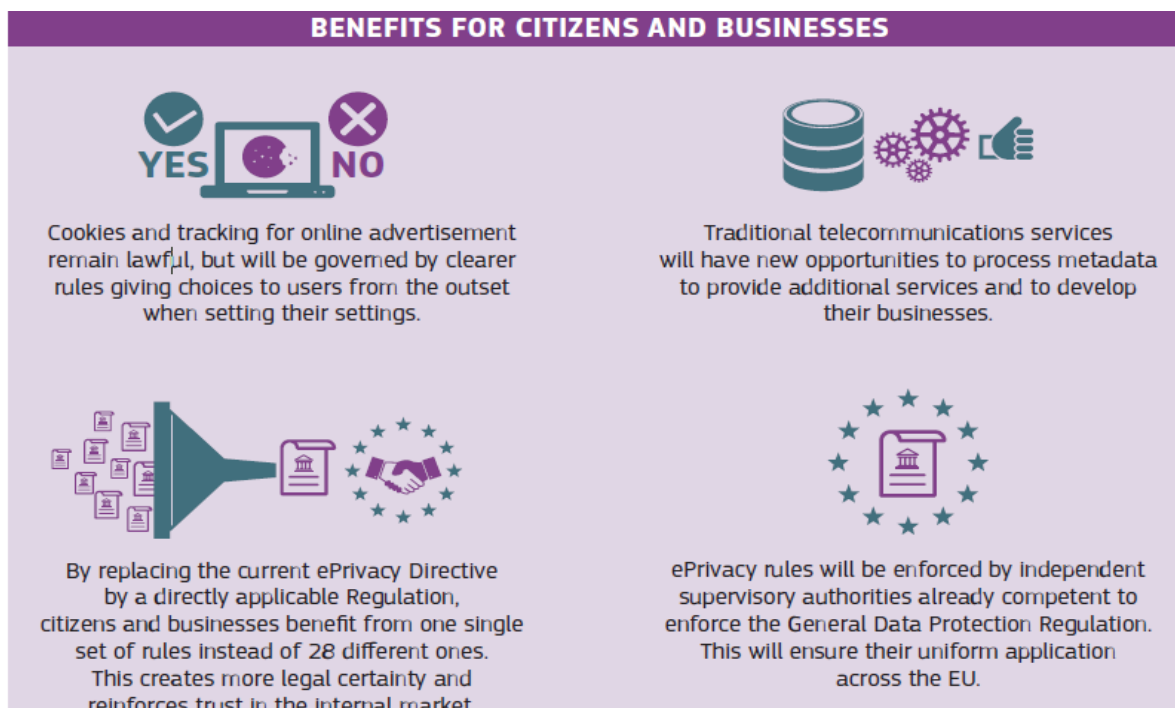
General Data Protection Regulation	Proposal for the ePrivacy Regulation
<ol style="list-style-type: none"> 1. Covers all personal data independently on the means of transmission.  2. Defines the right to personal data protection.  3. Introduces new rights for citizens and obligations for companies.  4. Starts to apply on 25 May 2018.  	<ol style="list-style-type: none"> 1. Covers electronic communications and the integrity of the information on one's device, independently whether it is personal or non-personal data.  2. Right to the privacy and confidentiality of communications.  3. Ensures that mobile apps or Internet services through which you communicate cannot intercept, record, listen into, or tap in your communications.  4. Proposed on 10 January 2017 and currently in the legislative process in the European Parliament and the Council. 

Source: European Commission (2016)

3.5. Benefits for citizens and businesses

According to the European Commission this regulation has some benefits for citizens and businesses. The main benefits for citizens and business can be seen in the next figure.

Figure 12 - Benefits for citizens and businesses



Source: European Commission (2017)

4. Personal data protection

According to the European Commission, personal data is any information that is related to an identified or identifiable living individual. In other words, personal data is any information that can be used to identify a person.

The EU privacy and data protection framework has two main regulations: GDPR and ePR.

The GDPR 2016/679 is an EU regulation on data protection and privacy for all citizens of the EU and also the EEA.

GDPR came into effect on the 25th May 2018 in each European country. 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, as a consequence, laws are consistent across the entire EU. GDPR requirements aim to create more consistent protection of consumer and personal data across all EU nations.

In addition, GDPR focus on ensuring that users know, understand and consent to the data collected about them. The GDPR protects personal data regardless of the technology (automated or manual processing) used for processing that data in accordance with pre-defined criteria. Also, it doesn't matter how the data is stored (for example video, paper, etc...), in all cases, personal data is subject to the protection requirements set out by the GDPR and ePR.

The ePR aims to provide a high level of privacy protection for users of electronic communications services and was proposed by the European Commission in January 2017 as a part of its digital single market strategy and will replace the 2002 ePrivacy Directive.

Although the basic data protection regulation is directly applicable as an EU regulation in each EU member state, it contains some opening clauses and leaves the national legislator some leeway as we will see in the following section.



4.1. What regulations complement the European regulations

4.1.1. Austria

The regulations applied concerning personal data protection are:

- **GDPR** - in **German Datenschutz-Grundverordnung (DSVGO)**;
- **ePR**;
- **Austrian Data Protection Act Datenschutzgesetz (DSG)** that supplements the GDPR;
- **Data Protection Adaptation Act 2018 and Data Protection Deregulation Act 2018** (two amendments to Data Protection Act) were adopted to implement these opening clauses and margins. The Data Protection Adaptation Act 2018 was published in BGBl I No. 120/2017 and the Data Protection Deregulation Act 2018 in BGBl I No. 24/2018 both came into force on 25th May 2018;
- **Data Protection Directive** is a directive for the area of Justice and Home Affairs based on directive is based on EU Directive (EU) 2016/680 of the European Parliament and of the Council of 27th April 2016 on the protection of individuals with regard to the processing of personal data by the competent authorities for the following purposes: prevention, investigation, detection or prosecution of criminal offences, enforcement of sentences, on the free movement of data and repealing Council Framework Decision 2008/977/JHA (Österreichische Datenschutzbehörde, 2019).

4.1.2. Czech Republic

In the case of Czech Republic the legislation applicable are as follows:

- **GDPR**;
- **ePR**;
- **Resolution No. 205** (15th March 2010) addresses cybersecurity issues and



has established the Ministry of Interior of the Czech Republic as a coordinator of cybersecurity issues and the national authority for the area;

- **Resolution No. 380** (24th May 2010) established the Interdepartmental Coordination Council for the area of cybersecurity;
- **Resolution No. 564** (20th July 2011) is related to Czech Cybersecurity Strategy for the period of 2011-2015;
- **Resolution No. 781** (19th October 2011) established the Authority as a coordinator for cybersecurity affairs as well as the national authority for the Cybersecurity area;
- **Cybersecurity Law** (1st January 2015) is directly related to cybersecurity issues;
- **Decree No 437/2017** (8th December 2017) transposes the relevant legislation of the EU and regulates sectoral and impact criteria for the determination of an operator of essential service and specifications for determining the importance of an impact of the disruption of an essential service on the security of social and economic activities;
- **Act No 181/2014 Coll** (19th December 2014) about cybersecurity and change of related acts were published in the Collection of Laws: Decree No 316/2014 Coll. on Security Measures, Cybersecurity Incidents and Reactive Measures ("Cybersecurity Regulation"); Decree No 317/2014 Coll. on Important Information Systems and their Determination Criteria; and, Governmental order No 315/2014 Coll. which amends the Governmental order No 315/2014 Coll. which amends the Governmental order No 432/2010 Coll. on the Criteria for the Identification of a Critical Infrastructure Element;
- **Decree No 82/2018 Coll** (21th May 2018) is connected to security measures, cybersecurity incidents, reactive measures, cybersecurity reporting requirements and data disposal (the Cybersecurity Decree).

4.1.3. Portugal

In Portugal, the personal data protection framework is regulated by:



- **GDPR;**
- **ePR;**
- **ePrivacy act** (29th August 2012) that should be applied to the processing of personal data in connection with the provision of public available electronic communications services in public communications networks, including public communications networks supporting data collection and identification devices, specifying and complementing the provisions of Law nº 67/98 of 26th October. Companies providing public available electronic communications services should establish internal procedures for responding to requests for access to user's personal data presented by the competent judicial authorities in compliance with the referred special legislation. Under the ePrivacy Act, the delivery of unsolicited communications for direct marketing is subject to prior consent of the subscriber that is an individual or the user;
- **Constitution of the Portuguese Republic (article 35)** that establish that all citizens have the right of access to any computerized data related to them and the right to be informed of the use for which the data is intended. Therefore, under this law, they are entitled to require that the contents of the files and records be corrected and up to date. This law determines what personal data is, as well as the conditions applicable to automatic processing, connection, transmission and use and should guarantee its protection by means of an independent administrative body;
- **Data Protection Act - Law 67/98** - (26th October 1998) which is the legal framework that generally applies to both private and public sectors as well as to any sector activity. Data Protection Act aims to protect an individual's right to private life while processing personal data establishing the rights and associated procedures of natural persons (data subjects) and the rights, duties and liabilities of legal and natural persons when processing personal data. The Data Protection Act also sets out principles and obligations that data handlers must comply with when carrying out personal data processing. The general principle of this law establish that the processing of personal data shall be carried out transparently



and in strict for privacy and for other fundamental rights, freedoms and guarantees;

- **Law 32/2008** (18th July 2008) which sets out the data retention obligations imposed on providers of publicly available electronic communications services. This law is related to the retention of data generated or processed in connection with the provision of public available electronic communications services or public communications networks;

- **Electronic communication laws - Law 5/2014** - (10th February 2004) and the **ePrivacy Law**. Under these laws, in the event of a security or integrity breach, these providers should notify the regulator (the National Communications Authority or ANACOM), the Comissão Nacional de Proteção de Dados and, in some circumstances, service subscribers and users;

- **EU Directive 2016/1148** concerning cybersecurity. Under this directive, there are measures for a high common level of security of network and information systems across the EU on July 2016. This directive allows the extension to other entities of the obligation to implement security measures and to notify security breaches.

4.1.4. Spain

In Spain, the personal data protection legislation that is applied are as follows:

- **GDPR**;
- **ePR**;
- **Lisbon Treaty (the charter of fundamental rights of the EU) and the Spanish Constitution of 1978** that are related to data protection and privacy and are both fundamental rights;
- **Several codes of conduct for data protection** that were approved under the former Spanish data protection regulations for various sectors;
- **Sector-specific regulations** that also include data protection provisions since certain categories of personal data and certain processing activities may require specific protection such as the processing of personal data within the financial, e-



communications or health-related sectors;

- **New Spanish Data Protection Law** (25th May 2018) provide specific data protection regulation in different fields that are not expressly included in the GDPR or that are included in the GDPR but with a scope that allowed for more detailed regulations to be introduced by the member states. Moreover, this law incorporates the Spanish legal system a list of new rights of citizens in relation to new technologies known as “digital rights”. This law also includes an amendment of Spanish General Electoral Law, allowing political parties to process of personal data for specific electoral promotional activities;

- **E-Commerce Law 34/2002 (LSSI)** and the **General Telecommunications Law 9/2014 (GTL)** that are related to sector-specific regulations may also contain data protection provisions;

- **Directive EU 2016/680** (27th April 2016) of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA;

- **Cybersecurity code** that brings together all the updated rules that directly affect cybersecurity. However, cybersecurity regulations still need further development.



In the next table, you find a brief summary of the personal data protection laws that are applied in Portugal, Czech Republic, Portugal and Spain.

Table 1 - Personal data protection legislation

	Personal data		Non personal data	Additional personal data legislation	Brief explanation
	GDPR	ePR	Regulation (EU 2018/1807)		
Austria	✓	✓	✓	Austrian data protection act Datenschutzgesetz	The Austrian data protection act (DSG) supplements GDPR
				Data Protection Adaptation Act 2018 (BGBl I No. 120/2017)	These two laws were adopted to implement the opening clauses and margins (in addition to amendments to numerous material laws) to the Data Protection Act. Also, these laws supplements GDPR
				Data Protection Deregulation Act 2018 (BGBl I No. 24/2018)	
				Data Protection Directive	This Directive is based on EU Directive (EU) 2016/680 of the European Parliament and of the Council of 27 th April 2016 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or of the enforcement of sentences, on the free movement of data
Czech Republic	✓	✓	✓	Resolution No. 205	Address cybersecurity issues and established the ministry of Interior of the Czech Republic as a coordinator of cyber security issues and the national authority for the area
				Resolution No. 380	Established the Interdepartmental Coordination Council for the area of cyber security
				Resolution No. 564	Czech Cybersecurity Strategy 2011-2015
				Resolution No. 781	Authority as a coordinator for cybersecurity affairs as well as the national
				Cybersecurity Law	This law regulates the cybersecurity in Czech Republic and it is in force since 1 st January 2015

				Decree No 437/2017	This decree transposes the relevant legislation of the EU and regulates sectoral and impact criteria for the determination of an operator of essential service and specifications for determining the importance of an impact of the disruption of an essential service on the security of social and economic activities
				Act No 181/2014 Coll	Related to cybersecurity and change of related acts to this topic
				Decree No 82/2018 Coll	Connected to security measures, cybersecurity incidents, reactive measures, cybersecurity reporting requirements, and data disposal (the Cybersecurity Decree)
Portugal	✓	✓	✓	ePrivacy act	Processing of personal data in connection with the provision of public available electronic communications services in public communications networks, including public communications networks supporting data collection and identification devices
				Constitution of the Portuguese Republic (article 35)	Establish that all citizens have the right of access to any computerized data related to them and the right to be informed of the use for which the data is intended, therefore, under this law, they are entitled to require that the contents of the files and records be corrected and up to date. This law determines what personal data is, as well as the conditions applicable to automatic processing, connection, transmission and use and should guarantee its protection by means of an independent administrative body
				Law 67/98 of 26th October	Legal framework about data protection act that generally applies to both private and public sectors as well as to any sector activity
				Law 32/2008 of 18th July	Sets out the data retention obligations imposed on providers of publicly available electronic communications services
				Law 5/2014 of 10th February and ePrivacy Law	Under these laws, in the event of a security or integrity breach, these providers should notify the regulator (the National Communications Authority or ANACOM), the Comissão Nacional de Proteção de Dados and, in some circumstances, service subscribers and users
				EU Directive 2016/1148	Allows the extension to other entities of the obligation to implement security measures and to notify security breaches

Spain	✓	✓	✓	Lisbon Treaty Spanish Constitution of 1978	Related to data protection and privacy and are both fundamental rights
				New Spanish Data Protection Law Law 3/2018 of 7th December	Provide specific data protection regulation in different fields that are not expressly included in the GDPR or that are included in the GDPR but with a scope that allowed for more detailed regulations to be introduced by the member states
				E-Commerce Law 34/2002 (LSSI) General Telecommunications Law 9/2014 (GTL)	Related to sector-specific regulations
				Directive EU 2016/680 of the European Parliament and of the Council of 27th April 2016	Protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
				Cybersecurity Code	States the main rules to be taken into account regarding the protection of cyberspace and to ensure the aforementioned cybersecurity

Source: Author's own elaboration



5. Non-personal data

Free flow of non-personal data means unrestricted movement of data across border and Information Technology systems in the EU.

The regulation on the free flow of non-personal data in the EU is already in force. The exact name for this regulation is regulation (EU) 2018/1807 of the European Parliament and of the Council of 14th November 2018 on a framework for the free flow of non-personal data in the EU.

This regulation aims to ensure the free flow of data other than personal data within the EU by laying down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users.

This regulation also applies to the processing of electronic data other than personal data in the EU which is:

- Provided as a service to users residing or having an establishment in the Union, regardless of whether the service provider is established or not in the Union;
- Carried out of a data or legal person residing or having an establishment in the Union for its own needs;

This regulation does not apply to an activity which falls outside the scope of Union law.

Figure 13 - Non personal data



Source: Business2Community (2019)

The guaranteeing free flow of non-personal data has the following principles across the EU:

- The free flow of non-personal data principle removes unjustified data localisation restrictions imposed by public authorities, enhancing legal certainty and raising trust;
- The principle of data availability for competent authorities makes sure that the data remains accessible for regulatory and supervisory control also when stored or processed across borders in the EU;
- Actions to encourage cloud services providers to develop self-regulatory codes of conduct for easier switching of provider and porting data back to in-house servers, which must be implemented by mid-2020;
- Security requirements on data storage and processing remain applicable, also when businesses store or process data in another member state. The same applies when they outsource data processing to cloud service providers;
- Single points of contact in each member states to liaise with other member states contact points and the commission to ensure the effective application of the new rules on the free flow of non-personal data.

The **GDPR and the regulation on the free flow of non-personal data will function together to enable the free flow of any data**, creating a common European space for data. These two regulations together create legal certainty for companies and guarantee that personal and non-personal data can move freely within the EU.

5.1. Free movement of data within the EU

Data localisation requirements shall be prohibited unless they are justified on grounds of public security in compliance with the principle of proportionality. Therefore, the member states immediately communicate to the commission any draft act which introduces a new data localisation requirement or makes changes to an existing data localisation requirement in accordance with the procedures present in articles 5, 6 and 7 of Directive (EU) 2015/1535.



In addition, the **regulation applied to non-personal data** ensures:

- **Free movement of non-personal data across borders:** every organisation should be able to store and process data anywhere in the EU;
- **The availability of data for regulatory control:** public authorities will retain access to data, also when it is located in another member state or when it is stored or processed in the cloud;
- Easier switching of cloud service providers for professional users. The Commission has started facilitating self-regulation in this area, encouraging providers to develop codes of conduct regarding the conditions under which users can port data between cloud service providers and back into their own IT environments;
- Full consistency and synergies with the cybersecurity package and clarification that any security requirements that already apply to businesses storing and processing data will continue to do so when they store or process data across borders in the EU or in the cloud.

Along with this regulation the GDPR already provides for the free movement of personal data. By 30th May 2021, member states have some rules regarding to data localisation requirements laid down on the basis of existing Union law.

5.2. Porting of data

The European Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level in order to contribute to a competitive data economy, based on the principles of transparency and facilitate the development of self-regulatory codes in order to contribute to a competitive data economy.

5.3. Procedure for cooperation between authorities

According to article 7, each member state shall designate a single point of contact which shall liaise with the single points of contact with the others member states and the Commission regarding the application of this regulation. This means that member states shall notify to the Commission the designated single points of contact and any



subsequent change.

5.4. Data availability for competent authorities

As regards to article number 5 this regulation shall not affect the powers of competent authorities to request or obtain access to data for the performance of their official duties in accordance with Union or national law. After requesting access to a user's data, a competent authority does not obtain access and if no specific cooperation mechanism exists under Union law or international agreements to exchange data between competent authorities of different member states, that competent authority may request assistance from a competent authority in another member state in accordance to article 7.

5.5. Penalties for breaches

This regulation lays out penalties for a breach which outlines different penalties for different infringements (the same sanctions that apply under GDPR also apply to the ePR). This means that penalties range from up to 10 millions euros or 2% of worldwide annual turnover for more serious breaches whichever is the higher in each case.

The eventual fines are heavily dependent on a number of mitigating factors, such as the scale of the incident, whether a breach of regulation occurred as a result of a deliberate act and how diligent the company was regarding the prevention of such incidents from happening.



6. Systematized content catalogue

Cybersecurity: is the practice of protecting systems, networks and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing or destroying sensitive information, extorting money from users or interrupting normal business processes.

Data Protection Act: independent public authorities that supervise the application of the data protection law. They provide expert advice on data protection issues and handle complaints against violations of the GDPR and the relevant national laws.

Data Protection Officer: the person responsible for monitoring and the application of data protection rules in the European Commission. A DPO is an employee within your organization who is responsible for understanding and ensures your organization's compliance. The DPO ensures the internal application of data protection rules in cooperation with the European Data Protection Supervisor.

ePrivacy Regulation: proposal from the European Commission designed to strengthen the protection of European Union citizens private life and create new opportunities for business.

GDPR: regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area. It also addresses the transfer of personal data outside the European Union and European Economic Area.

Non-personal Data: electronic information that cannot be traced back to an identified or identifiable natural person (or has been anonymized as such).

Personal Data: any information that relates to an individual who can be directly or indirectly identified. Names, photos, geographical information, web cookies, email address are some examples personal data.



7. Conclusions

Data protection and cybersecurity are becoming essential values for society and, because of that, these two areas have recently undergone significant legal development and are more consolidated in the EU.

The regulation for dealing with personal data differs from the regulation for the non-personal data in EU member states. However, the regulations that concerns to the non personal data and personal data is the same for all member states. In this context, regulation (EU) 2018/1807 applies to the free flow of non-personal while with regard to data protection, as in all other EU jurisdictions, the main rule is the GDPR. Along with the GDPR the regulation related to the free flow of non-personal data will function together to enable the free flow of any data that will result in a common European space for data.

In addition, the ePR sets some rules related to the protection of privacy in the electronic communications sector. In particular, this regulation applies to providers of electronic communications networks and services and was due to come into force on 25th May 2018, alongside with the GDPR however continued deliberation and lobbying of some of its finer have delayed the application of this regulation. The ePR doesn't contain an explicit provision with regard to the applicable national law which creates legal uncertainty as to which law should apply in a cross-border context.

Nevertheless, although the basic data protection regulation is directly applicable as an EU regulation in each EU member state, it contains numerous opening clauses and leaves the national legislator some leeway.



8. References

Business2Community (2019). Why User Data is the Next Big Deal in Digital? Retrieved from <https://www.business2community.com/mobile-apps/why-user-data-is-the-next-big-deal-in-digital-02179282>.

Deloitte (2019). The GDPR: Six Months after Implementation. Retrieved from <https://www2.deloitte.com/bg/en/pages/legal/articles/gdpr-six-months-after-implementation-2018.html>.

EU GDPR.ORG (2019). The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years. Retrieved from <https://eugdpr.org/>.

European Commission (2019). Complete guide to GDPR compliance. Retrieved from <https://gdpr.eu/>.

European Commission (2019). Data protection under GDPR. Retrieved from https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm#shortcut-3-who-monitors-how-personal-data-is-processed-within-a-company.

European Commission (2019). Eurobarometer on ePrivacy. Retrieved from <https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy>.

European Commission (2019). Free flow of non-personal data. Retrieved from <https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data>.

European Commission (2019). General Data Protection Regulation: one year on. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2610.

European Commission (2019). Proposal for a regulation on privacy and electronic communications. Retrieved from <https://ec.europa.eu/digital-single->



[market/en/news/proposal-regulation-privacy-and-electronic-communications](https://www.market/en/news/proposal-regulation-privacy-and-electronic-communications).

i-Scoop (2019). Data processing principles: the 9 GDPR principles relating to processing personal data. Retrieved from <https://www.i-scoop.eu/gdpr/gdpr-personal-data-processing-principles/>.

ITPRO (2019). ePrivacy Regulation: What is it and how does it affect me? Retrieved from <https://www.itpro.co.uk/privacy/32712/eprivacy-regulation-what-is-it-and-how-does-it-affect-me>.

Serve IT (2017). GDPR for developers - data subject rights. Retrieved from <https://www.serveit.com/gdpr-for-developers-data-subject-rights/>.

