CAN GDPR CHANGE MARKETING? HOW DIGITAL MARKETING CAN REACT TO SUBJECTIVE OBSTACLES

Luís Requicha, Instituto Universitário de Lisboa (ISCTE-IUL)
Mário Nuno Mata, ISCAL-IPL: Instituto Superior de Contabilidade e Administração de Lisboa, Instituto Politécnico de Lisboa
José Moleiro Martins, Instituto Universitário de Lisboa (ISCTE-IUL)
Pedro Neves Mata, Instituto Universitário de Lisboa (ISCTE-IUL)
Anabela Batista Correia, ISCAL-IPL: Instituto Superior de Contabilidade e Administração de Lisboa, Instituto Politécnico de Lisboa
Rui Miguel Dantas, ISCAL-IPL: Instituto Superior de Contabilidade e Administração de Lisboa, Instituto Politécnico de Lisboa

ABSTRACT

There is a long way to go in practices and culture regarding the protection of personal data. There is a somewhat deficient and different implementation.

Some companies have implemented detailed internal procedures, restructured and renewed the content of the databases, bet and invested in the most varied applications and services for massive e-mail sending. Helping one side to a widespread bet on new products, and the other side, to apply and improve by some service providers in their marketing tools - with a common objective: to guarantee a management capacity and demonstration of consent. For the GDPR, you can start a new beginning: with the decision to recover the total number of databases and guarantee the legitimacy for sending future electronic communications (direct marketing). Other significant ones for the development of new strategies, is to reverse the loss of data numbers. If it is true that consent was and remains the most widely used license basis for processing personal data, it is also true that companies often continue to require or consent from holders, when it is not allowed or allowed, creating a wrong test citizens that everything is dependent on their consent. The inevitable consequence: the holders project a right to withdraw a consent that is not actually necessary to have given. This factor does not generate a title claimed for something that, in fact, is not legally supported.

Keywords: General Data Protection Regulation (GDPR), Marketing, Digital Marketing

INTRODUCTION

With the General Data Protection Regulation (GDPR) there is a need to better understand the customer's data assets (the data subject) and where they reside within any organization.

The implementation of an adequate compliance process, together with a targeted marketing strategy for information management and efficient databases, presents itself not only as an opportunity for innovation and competitiveness for businesses, but confidence booster too and reputation of the brand.

Lately, when acceded to a website, we are faced with a new box to warn us about the creation of cookies. This change happens because of the implementation and expected changes in the Data Protection General Regulation, the GDPR, which entered into force on 25 May 2018.

This regulation rather changed the responsibility of professionals who handle the personal data of EU citizens. The main objective of this regulation is to increase security and protecting the privacy of online users. Thus, the GDPR has required a series of measures with regard to the processing and analysis/use of data in order to make all this more secures, transparent and confidential.

More importantly, the user or client to control the consent, collection, processing and forms of use of their personal data. For example, subscribing to a newsletter, previously asked only for the user/client to write your e-mail in the signature field. Now the lead is, after subscription, receive an email confirmation.

To remember: Failure of GDPR could lead the company to be punished with a fine up to 4% of its annual revenue.

In essence, the GDPR is a safeguard consumer. Basically, it is sure that users are free to deliver their data only to those who want and even when they deliver them, remain the owners, and can change them or remove them so wish.

It is important to remember that the data of consumers and users of services are super valuable in shaping the digital marketing strategies, for example. With a correct treatment of data, you can define the persona and therefore predicting their preferences, behavior and future attitudes.

Every day, there are doubts and questions, such as: the new rules of this regulation will be a problem for my company? Well, if you work with digital marketing and does not have a strategy and you are only concerned with selling, no doubt that will be a problem.

But if the digital marketing is strategic and planned in order to follow the target audience in its various stages, will not be.

In short, from now on, with the new data protection law, GDPR, companies actually have to collect the data in a legitimate manner and to ensure consumer rights with regard to the analysis and use of your personal data.

Of the various changes implemented, the most relevant are:

- "Breach Notification" - That is, in case of violation of personal data, shall be the obligation and the need to communicate with the competent authorities and the affected consumers, within 72 hours;
- "Right to Access" - guarantees any person the right of access to their personal data, and request a copy of all data that is held by the organization;
- "Right to be Forgotten" - This is the right to be forgotten, by requesting the deletion of your personal data directly to organizations, should this right be granted with as soon as possible;
- "Data Portability" - This is the right that the consumer must request that their personal data is transmitted to another entity;
- "Data Protection Officer" - This is to ensure that companies have human resources record and maintain an effective data protection.

The consent of the person who provides personal information to be carried out in a clear and direct language with no room for second interpretations. Therefore, one should analyze the use and privacy policy that you have available on the site.

The GDPR requires that for all data processing, consent is explicit.

So, what is the Data Protection General Regulations, in the broader context?

The General Data Protection Regulation (GDPR) or "General Data Protection Regulation" (GDPR) - Regulation (EU) No 2016/679 - is a legal framework of the European Union (EU) that applies to all Member States members and any other country that sells products or services in Europe.

In force since May 24, 2016, but shall apply from 25 May 2018, aims to protect individuals with regard to the processing of personal data and on the free movement of such data.

In practical terms, any company based in the EU or outside the EU, in the context of activities that exercise (even for free), treat personal data of citizens living in Europe, collected

by automated means (or not automated), is obliged to report on all actions involving this treatment and about the privacy policies given to people who supplied them.

Thus, all personal data processing activities must be recorded in detail: which data are stored, as they are registered, that are used as they are handled, stored, and for how long.

Since it is not a directive, but a regulation, the GDPR is mandatory and binding legal power.

The GDPR replaces Law No. 67/98 of October 26, and the subsequent on Personal Data Protection, 2003.

In addition to requiring that obtaining consent from the user - to receive any kind of communication or processing of personal data by a company - it is a totally clear and transparent, the main changes from the previous legislation are following:

- The citizen has the right to "be forgotten";
- You have the right to information;
- You have the right of access;
- You have the right to rectification;
- You have the right to the limitation and treatment of opposition;
- You have the right to portability;
- You have the right not to be subject to automated individual decisions.

The new Data Protection General Regulation is the most important change in the privacy of adjustment data from the last 20 years and, in very general terms, aims to strengthen the fundamental rights that individuals have over their personal data and, in the background, prepare Europe for the digital age.

It is recalled that the Community Directive into force before the GDPR was created before the era of social networks or even before the world has become increasingly global and connected to the network. 1995 was the year when Microsoft introduced Internet Explorer or one that Amazon and eBay were founded. The number of Internet users was around 16 million.

In acceleration of historical process and already in 2018, more than 3.7 billion users. Mobile devices - smartphone, tablet, smartwatch, laptop, among a number of other gadgets - longer function as an extension of the body, so is the need for connection to the network - access, contact, exposure, consumption, Communication.

The dimension of this cultural transformation was necessarily a huge economic impact. In the digital society, facilitated access to citizens became effective gold in business. Aware that their customers share the need to be always connected, companies are the main interested in understanding who they are or what are the behavioral tendencies that their targets have online.

The new Regulations have thus relaunch the discussion on the protection of personal data, but also on issues of privacy, encouraging critical thinking about how citizens provide their data and how often "give up "of his rights to have access to online services.

Offer up personal data - name, address, email address, phone contacts, location, photos, and credit card details, among others - and themselves accept, uncritically, terms and confusing privacy policies for access to content and services.

On the one hand, sharing this type of data is used to create relationships with organizations with which we interact and are part of our day-to-day. On the other, if this information falls into the wrong hands, it can be used for a number of fraudulent activities, including identity theft.

It will not be exaggeration to say that a major 'gaps' of the previous Directive held up, so to speak, with the lack of metrics for the application of the rules of data protection. Each Member State interprets those rules in their own way when changed into local legislation.

The nature of GDPR has thus intended to strengthen data protection laid down in the Charter article 8 of the European Union Fundamental Rights and harmonize existing legislation

in the Member States, laying the foundations for the single market digital. The EU believes that the new legislative framework will save collectively, many millions of euros per year.

In short, this regulation is an essential measure to reinforce the fundamental rights of citizens in the digital age and to facilitate commercial activity through the simplification of rules applicable to companies in the digital single market. The introduction of a single legislative act also end the fragmentation and costly administrative burdens that currently exist.

As it reads in the new Data Protection General Regulation, the new legislative framework aims to "contribute to the realization of an area of freedom, security and justice and of an economic union, to economic and social progress, the consolidation and the convergence of economies within the internal market and for the welfare of individuals".

Therefore, the GDPR aims:

- Ensure respect for the fundamental right of every person to privacy of your data;
- Protect EU citizens in a global economy context;
- Give citizens full control over their personal data;
- Harmonize existing legislation in Member States;
- Halting the growth of online leaks, loss of confidential data and cyber-attacks;
- Strengthen the protection of enterprise systems.

Transparency, clarity, access, consent, right to opposition are some of the concepts aimed at the empowerment of citizens in regard to the use, handling and sharing of personal data by business organizations.

The process in accordance with the new legislation will require companies considerable effort in terms of compliance with the new rules. In addition to being required to revise a number of organizational measures and techniques for data processing, there is also a mindset work for their employees who will necessarily be carried out.

Among a wide range of measures, companies will, for example:

- Adopt security mechanisms of personal data;
- Provide training to employees about GDPR standards;
- Assess the need/requirement to appoint a Data Protection Officer (DPO) or Data Protection Officer, figure responsible for managing the compliance process within the company;
- Map and categorize the personal data collected and processed;
- Create automations that simplify compliance with the Regulation;
- Report to the regulatory authorities and the respective owners of the data the occurrence of incidents of data breach within 72 hours after being known a security breach.

FRAMEWORK

The new regulation applies to all organizations established in the European Union and those which, being located outside the EU treat data residing citizens, since they market their products/services (for consideration or free) or monitor behaviors that occur within the EU.

It is noteworthy that are excluded from this requirement, for example, the public security forces, since they are subject to specific legislation.

Importantly to note that, with regard to the detailed record of the data processing activities, business organizations with fewer than 250 employees are excluded from this requirement, provided that if none of the following conditions in data processing:

- Is likely to present a risk to the rights and freedoms of the data subject;
- There is occasional;
- Covers the following categories of data: racial/ethnic, political, religious, philosophical, trade union membership, genetic, biometric and health, sex life and sexual orientation;
- Personal data connected with criminal and convictions.

Compliance with the GDPR wills supervision in Portugal by the National Data Protection Commission (CNPD), with this help and constant each of us, personal data holders.

At the same time, consent has become one of the most important requirements for the processing of personal data can be considered legal. And even when consent to treatment is given by the owner, there are many constraints to take into account so that companies can carry out this treatment. This is because, according to the GDPR, citizens now have the following rights:

Right to Information

All citizens have the right to receive information about the terms that involve the processing of personal data contract.

Do not just give access to endless information pages with small print and difficult to understand letters.

Information must be clear, brief, expressed in a language easy to understand and distinguishable from other information such as the terms and conditions. It is considered that only then the consent may be informed.

It should also be noted that companies are required to notify the national supervisory authority (National Commission for Data Protection) when there is a data breach that put the owners of the data at risk in the next 72 hours period to the notice of violation. They must also communicate to citizens affected so that they can take appropriate action.

Right of Access

This is another reference aspect of the new Regulation. Citizens will have access to more information about the data and how they are processed. This information will need to be clear and accessible. After consent, citizens can access the data that is collected and confirm what they are and if they are being, or not subject to treatment. Companies must create ways for such access is easy and fast, and many already allow this online consultation.

Right to Oblivion

Citizens go on to have the right to "be forgotten." That is, has the right to request that their personal data to be deleted without undue delay and within the legally prescribed limits.

This right only leaves out the data that are necessary for companies to comply with their legal obligations. For example, it cannot be used to erase data that impede the collection of debts.

The measure, according to the GDPR, aims to "protect the privacy of individuals, not erasing past events or restrict the freedom of press."

The Regulation also states that "the holder has the right to obtain the deletion of your personal data and the organization has the obligation to do so without undue delay when you apply one of the following reasons:

- Personal data no longer needed for the purpose for which their collection or treatment;
- The holder withdraws the consent that is based on the processing of data, if no other legal basis for such treatment;
- The opposition to the treatment holder and there are no prevailing legitimate interests justifying its treatment;
- Illegality with the processing of personal data;
- Personal data should be excluded in order to comply with the legal obligations of the EU or a Member State, where the controller is obliged;

- Personal data collected in connection with the provision of information society services".

Correction Right

If the data subject finds that the personal information is inaccurate, he is entitled to, without undue delay, get your correction or update.

For example, where the family situation and work may have already been changed or where the disclosure of the former situation can be embarrassing or even harm the life of the holder.

Right to Data Portability

New right to data portability will make easier the transmission of personal data between service providers. This is because citizens now can transfer your data to another service provider whenever you want.

In addition, any citizen can request delivery of their data in current use and machine-readable format - either to archive or to work your own information.

Right to Limitation and Treatment of Opposition

Given consent to the processing of personal data, the holder may at any time request the limitation of full or partial treatment of your data, without for such a contracted relationship with the company will be affected.

Very useful, for example, prevent unwanted direct marketing by a supplier, keeping the other aspects of the business relationship.

The holder also has the right to object to the disclosure or sharing of personal data.

Right to Protection of Data "by Design" and "by Default"

Data protection "by design" means that each new service or business that makes use of personal data is required to take into account the protection of such data. In this respect, companies must be able to show that they have appropriate security.

In practical terms this means that information technology departments must take into account the privacy of data on the "design" of the product or service technology. "By design" means that companies will have to make sure that only the absolutely necessary personal data for a given action will be prosecuted.

Citizens' data privacy settings should be, by default, at the highest level of security.

In addition, personal data must, by definition, only be maintained as long as necessary space to provide specific product or service.

Responsible for Data Processing *vs.* Subcontractor

According to the information provided by the UE, the data controller ("Controller") determines the purposes and the means by which personal data are processed.

A company/organization is responsible for the treatment is decided "why" and "how" human information processing. Workers who perform the processing of personal data in the organization do it to fulfill the tasks while the controller.

However, a company/organization are also responsible for the set treatment when determining, in conjunction with one or more organizations, "why" and "how" personal data

must be processed. Responsible sets the controller may conclude an agreement defining the respective responsibilities for compliance with GDPR rules. The main aspects of this agreement shall be communicated to the persons whose data are subject to treatment.

Since the processor performs only the processing of personal data on behalf of the controller (“processor"). The processor is usually external to the company. However, in the case referred to enterprise groups, a company can act as subcontractor for another company.

CONTEXT AND DIAGNOSIS

The GDPR has direct application from 25 May 2018. The Regulation entered into force on May 24, 2016, after nearly five years of negotiations and about 4.000 additions, being applied directly, *i.e.*, without any transposition into national law.

Given the above, we understand that the implementation of GDPR involve several changes in the digital marketing strategies of companies. In particular:

Decrease of Databases

The more explicit for the necessary user permission, and the simpler the cancellation of the access of companies to these data, the more complicated it will be to generate and expand the databases, especially when for use of third parties (such as the companies that sell databases).

Range Limit Certain Channels

There are numerous digital marketing strategies (such as cookies and remarketing) that were not based on the explicit consent of the consumer.

Thus, the smaller the audience, the smaller the range obtained.

Increase in Cost Click

Another indirect impact of GDPR passes essentially the average price per click for paid advertisements (including Google and Facebook).

The need to insert the new databases on third-party advertising platforms makes the process more expensive.

It should be noted as well that with the implementation of the new data protection law, companies must implement a digital marketing strategy in the medium and long-term focus.

Therefore, investment in SEO, content marketing, inbound marketing and everything that allows to your company strengthen relationships with are customer effectively the strategies that your company should focus immediately, because they are the ones the medium and long term will bring a greater return for your business.

The impact of GDPR in email marketing: after all, there is a reward!

Six months after the General Data Protection Regulation (GDPR) comes into force, the benefits of compliance are already notorious. After all, there is a reward!

Contrary to what many companies may think, the GDPR came not to complicate the lives of marketers or as required of campaigns and email marketing. On the contrary! It is a law that helps clear the databases and, consequently, will direct their efforts to the right target.

At first it may seem impertinent respect GDPR, but that's because it is not to have a long-term vision. It is understandable that you are not comfortable to erase all contacts who have not

given consent, but better take a step back, then give two ahead ... a good leader has to have lynx eyes.

But after all, what are the benefits to meet the GDPR? Now share the BMW success story, the You Lead client:

- Engagement rates never seen before: to comply with the laws of GDPR, BMW is now communicating to people who actually want to be connected to the brand! The end result will be open rates and amazing conversion rates (the last campaign email marketing BMW achieved an open rate of 61.67 %!);
- Customer confidence: Due to the transparency of the approach during the opt-in campaigns, BMW customers are now more loyal to the brand;
- Increase ROI: If there is a better performance in e-mail marketing campaigns, there are more and better conversions. Thus, BMW is able to get more return on the investments made in e-mail marketing, and ultimately creating a better brand image in the market.

Only it depends on you having a fully compliant company, but have everything in digital format will take you a lot of headaches because it will improve their conversion processes, while it is fulfilling GDPR.

DISCUSSION

According to GDPR, company/organization should be responsible for complying with all the principles of data protection and also for demonstrating such compliance (Principle of Responsibility).

In this respect, the new regulation provides companies/organizations a set of instruments, some of which required that allow them to demonstrate their responsibility.

For example, in specific cases, the appointment of a Data Protection Officer (DPO) or making Data Protection Impact Assessments (AIPD) may be required.

Data controllers may choose to use other instruments such as codes of conduct and certification procedures to demonstrate compliance with the principles of data protection.

Both codes of conduct and certification are optional tools, so it is up to the company/organizations decide whether to adhere to a certain code of conduct or seek certification.

Although the company/organization will continue to have to respect and comply with the GDPR, adherence to these instruments can be taken into account in the case of an implementing measure adopted against your organization for breach of GDPR.

But how is that marketing can be relearned and managed?

The defense of ARCO rights and freedoms of individuals with regard to the processing of personal data requires the adoption of appropriate technical measures and organizational, to ensure compliance with GDPR requirements.

The controller must adopt guidelines, such (include) as:

- Update rules | Which should reflect all of the company's shares to comply with the new legislation. You should include a list of all employees who handle personal data and respective responsibilities of discrimination.
- Reformulation of Terms and Conditions and Privacy Policy | Companies should review the Terms and Conditions and Privacy Policies of its online pages - which mostly are very extensive and confusing to the user. In addition to reflect the new data protection policies should be more transparent and concise.

- Evaluation of data collection | Companies should assess whether any information they collect from their customers is absolutely necessary.

If there is no clear justification for collecting and processing this data, it is advisable that companies not collect. All data that they collect should be mirrored in the rules, and the grounds of having collected and how to treat them.

Remember that you should collect and process personal data only for lawful purposes, and always protect this data. The safety requirements include prevention of accidental or criminal destruction, loss, processing, distribution, access and change. In other words, these requirements must ensure, among others, the ARCO rights.

- Assessment of the need to appoint a DPO - Data Protection Officer | Either a controller or a processor, if the main activities of the company/organization involved the processing of sensitive data or if the main activities involve the systematic, regular and large scale of people, then it should be named an EPD. This figure, which can be an employee or an external consultant, will be responsible for compliance with data protection matters.
- Employee training | In order to ensure non-violation of the new rules and to demonstrate that data protection is a matter of vital importance for companies, one of the many challenges will be, for sure, to sensitize employees to the new issues of privacy and treatment data. What is sought is to establish a new corporate mindset to this new era of regulation of privacy. It should additionally be completed terms of responsibility towards employees who have access to data personal.

One of the cross points to GDPR relates to the fact that companies have to keep documentation that proves, in case of inspection or audit, that all necessary consents have been collected and is in fact in accordance with the law.

You must keep documentation of all data processing activities, including the purpose of the processing, the categories of personal data involved, the categories of recipients, the safeguards on all data transfers, and if possible, time limits to delete these Dice.

It is also necessary to maintain a technical description of security measures in the organization.

These records shall be kept in paper or electronic, and available for audit and review by the supervisory authority when requested.

Consents | Although personal data processing rules in force in the law since 1995, are not very different in GDPR, the new regulation brings new requirements regarding the validity of the consent. In order to comply, companies must:

- Assess whether the data already collected and that are registered in the database were collected with the necessary consent. If not, the consents should be captured again in order to continue to communicate with their customers;
- Ensure that the platforms that are being used allow for a consent management. It is important that the user can manage their consent or even delete your account in your customer area at any time;
- Ensure that consent is obtained through an unambiguous positive act and a freely given specific, informed and explicit (e.g., consent may not be pre-selected in the case of using checkboxes);
- Ensure that consents are collected in granular form (e.g., so that the consent for different marketing activities must receive separate consents). In this regard, it should be remembered, consents cannot be referred to the terms and platform conditions, it does not serve as consent to collect evidence if the user do opt in (the act by which the user gives his consent);
- To favor consents obtained through double opt in. This is in addition to the consent cannot be "previously clicked", it is recommended that companies obtain a double consent. In practical terms, it translates to send an email to the data subject consents to confirm that, in fact, with these communications. This applies, for example, in cases of registration in the newsletter or register on the site, where the customer will receive an email to confirm that it was he who, in fact, made that record.

A request for consent must be presented in a clear and concise manner, using an easy to understand language, and in a way that clearly distinguishes it from other information such as Terms and Conditions.

The request must specify what use will be given to personal data and must include the company's contacts that perform data processing.

Approval must be free and be explicit. This means that the data subject must receive at least the following information about treatment:

- The identity of the organization conducting the processing of data;
- The purposes for which the data are being processed;
- The type of data to be processed;
- The possibility to withdraw consent given (for example, sending an e-mail message to withdraw consent);
- If applicable, the fact that the data going to be used exclusively for automated decisions, including profiling;
- Information to determine whether the agreement is related to an international transfer of data, the potential for data transfers outside the EU, if such countries are not subject to an adequacy decision by the Commission and there are no adequate safeguards.

Cookies | Until the entry into force of GDPR, the cookies were treated with a simple warning, acceptance or non-acceptance of cookies policy - to be able to continue browsing a particular website.

While cookies are not considered directly, personal data, there are ways of crossing of information that may lead to the identification of a citizen. For this reason, the GDPR sees the cookies as personal data, even if only indirectly identify a good citizen.

In this context and with a view to compliance, companies must:

- Making management cookies to allow the possibility for the user to accept or decline, some or all of the cookies. Each type of cookie must be explained to the user clearly and succinctly.
- Never refuse access to the same user that this refuse all cookies;
- While the user does not take any action on cookies, the site should not record any cookie in your browser, and it is advisable that the alert remains visible until the users take some action

.

Data base | The main concern that companies should have with their customer databases relates to the collection of consents. According to GDPR:

- The databases should be collected by companies in accordance with the rules of the new Regulation;
- It is advisable encryption of databases, to prevent cyber-attacks and/or any leaks of information. In case of leakage or theft, companies will have to alert within 72 hours the regulatory authorities and, in some cases, the actual members of the data;
- In the event of exercise of ARCO rights, should the databases be updated as intended right, depending on whether exercised the right of rectification, cancellation, opposition or oblivion.

As will be aware of each of us, the new Regulation requires that all security breaches that result in risk to the rights of holders to be notified to the supervisory authority as well as the respective holders of the data.

According to the new regulation (Article 33), in case of violation of personal data, procedures for communication to the supervisory authority are as follows:

A Privacy Policy is a document to be contained, for example, on the site of a company. Aims to inform transparently, fairly and clearly the users of that site about the data that is

collected, what they are used, with whom the data is shared (if applicable) and how the user can enforce their rights.

CONCLUSIONS

Penalties for those who are not in compliance with the new Regulation will be severe. The GDPR establishing a fines application framework built on two levels (due to gravity), namely:

- In less serious cases, the penalty may have a value up to 10 million or 2% of the annual turnover worldwide, whichever is higher.
- The amounts of 20 million or 4% of annual revenue can be applied as legal maximum fines.

In the first case, the fines fault will be applied in compliance with technical or organizational requirements, for example, failure to communicate breaches of their databases, or lack of certifications.

In the second, for the cases most serious violation of the basic principles relating to data security, for example, non-compliance with the consent given by the user, the transfer of personal data to other countries or organizations which do not ensure a certain level data protection.

REFERENCES

National Data Protection Commission. (2018). Regulation No. 798/2018. Official Gazette No. 231/2018, Series II of. 32031 - 32032.

EUR-Lex. (2018). The general data protection regulation applies in all Member States.

Wanda, P. (2018). Are consumers concerned about privacy? An online survey emphasizing the general data protection regulation. *International Conference on Project MANagement/HCist - International Conference on Health and Social Care Information Systems and Technologies*.

Wanda, P. (2018). Procedia computer science. *Hanne Sorum; Procedia Computer Science*, *138*, 603–611.

Steve, M. (2016). *Data protection: Prepare now or risk disaster (1st Edition)*. Computer Fraud & Security.

Christina, T., Anna, R., & Jouni, M. (2018). EU general data protection regulation: Changes and implications for personal data collecting companies. *Computer law & security review, 34*, 134–153.

Rob, P. (2018). GDPR – project or permanent reality? ASG Technologies. *Computer Fraud & Security, 1*(1), 1-10.

Tomi, M. (2014). Perceptions of controllers on EU data protection reform: A Finnish perspective. *Computer law & securityreview, 30*(190), e195.

Jay, P., Doh-Shin, J., & Byung-Cheol, K. (2010). Privacy and personal data collection with information externalities. *Journal of Public Economics, 1*(10), 36-46.

Maxine, G. (2010). *Revisiting the relationship between public relations and marketing: Encroachment and social media*. Public Relations Review; Elsevier.

Jef, J. (2018). *"Finding the missing link in GDPR compliance"*. Senzing.

Information Commissioner's Office (ICO). (2018). Data security incident trends.

Regulation (Ec) No 765/2008 of the european parliament and of the council of 9 july 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing regulation (EEC) No 339/93.