ABSTRACT

GDPR (General Data Protection and Regulation) is a framework on data protection and privacy policy of the individuals of the European Union and European Economic Area. The regulation seven years in the making finally comes into effect on 25 May and is set to force changes in everything from technology to advertising, and medicine to banking. GDPR is directly applicable in all EU member states from May 2018. It replaces the EU's previous law governing data protection. GDPR is introduced to protect the personal data of the individuals of the Europe. The main aim of the GDPR is to provide the citizens control on their own personal data. There is a need to the individuals to understand how their personal data is being used and controlled. This regulation aims to protect and safeguard the EU personal data. This will also clarifies how the companies which are processing personal data safeguard the data from any illegal activity.

KEY WORDS:

GDPR, Personally Identifiable Information (PII), Data Subjects, Data Controllers, Data Processors

1. INTRODUCTION

GDPR will allow the individual to have control over their personal data. That means whenever a person wants to demand his personal data, the company should give his data and if the person wants to delete the data the organization should do it.

This framework includes a set of rules which will define how the data of the individuals will be controlled, collected, stored, deleted and transferred. The data of the individuals include Personally Identifiable Information (PII) like name, email, passwords, profile photos and bank details etc. This also includes the posts on the social media and sometimes the IP addresses and cookies. Before the GDPR there is no guarantee for the protection of our data. Data Protection Officer (DPO) was not mandatory for the organization. Some organizations may send the data to others without our concern. Some may misuse the data and try to send spam emails and messages. This may lead to data breach.

Before the GDPR the privacy policies of the Businesses were in a lengthy format. They were in complicated terms which cannot be understandable by all the users. Businesses also thought that

users silence is the consent to the data processing. But that should not happen there should be an affirmative consent from the user before the data is processed. They should ask the users for their consent and should clearly indicate them what use will be made with that personal data. The users might not be informed when their data is transferred. They might be unaware of it. The businesses might have taken the permission for the data usage for one purpose and might used it for some other purpose. The data should be collected and processed only for well-defined purposes with the user consent. Some businesses might use algorithms to make decisions about the user based on their personal data. (E.g. when applying for a loan). The user should be informed whether the decision is automated or not and the user should be given the possibility to contest it. Often the businesses would not inform the users when there is a data breach or when the data is stolen.

The businesses and organizations should inform the users without any delay in case of harmful data breaches or attacks. Before the GDPR the users cannot take their data and move it to the another competing social media platform. It was difficult or sometimes it was not possible for the user to access their data. The users were unable to get a copy of their data what businesses or organization keep about them. It was a difficult task for the users to delete their data. Before the GDPR the data protection authorities had limited powers and means to cooperate, provide guidance, interpret and adopt binding decisions. If the company violates the data protection rules the authorities had a limited or sometimes no fine. But after the GDPR, if the organization violates the rules, it should pay up to 20 million EUR or 4% of the company's world wide turnover.

Confidential data like passwords may be protected but some of the details like name, email etc will be misused without our concern. This is done without bringing to our notice. After the GDPR, we have control on our data. If we want to delete the data the organization has to do it for sure. In some cases the data can be used without our concern. That is like medical purposes or some forensic organizations. Even to do this there should be a specific reason and it should be a valid one. The DPO who has a certification in GDPR is mandatory. He should take care of the data and its privacy.

Issues raised before GDPR:

- Lack of consumer confidence.
- Before GDPR data management was a problem. That means if the organization have GDPR compliance, then the data will be audited and the redundant data will be cleared and will be organized in a proper manner. This will even reduce the data.
- Before GDPR data protection (DPO) was not mandatory. Some companies' hire DPOs and some may not. But after the GDPR this is a mandatory one.
- Data maintenance cost was more.

2. MATERIALS AND METHODS

The Key stakeholders in GDPR are:

1. Data Subjects

This includes the collection and processing of any person's personal data

2. Data Controllers

This comprises the person who determines the purpose and methods for processing the data.

3. Joint Controllers

Two or more controllers jointly determine the purposes and methods of processing the data.

4. Data Processors

The person or company who processes the data based on the instructions of the controller.

5. Data Sub processors

This includes the third party individual or business which performs data processing for other companies.

6. Supervisory Authorities

Public authorities who monitor the applications of GDPR

Privacy by design

The ultimate aim of privacy by design is building privacy and data protection in the architecture and design of the ICT to ensure the privacy and data protection principle.

Privacy by design focuses the data protection through technology design.

1. Personal Data

Personal data refers to the personal information such as name, location, identification number, physical address, email address, video, video recording, biometric data, online identifier etc.

2. Profiling

Any form of automated processing of personal data to evaluate personal aspects.

3. Processing

Processing defines the set of operations performed on set of personal data.

4. Recipient

The personal data are disclosed to the public authority or agency.

5. Data Concerning Health

The personal data related to the mental or physical health of a person.

The Impact of GDPR:

The hardest hit might be those that hold and procedure massive quantities of consumer information:

1. Technology corporations

2. Entrepreneurs

3. The data brokers who join with them

4. The impact of GDPR on customer engagement

Impact on Business and Technology Corporations

GDPR impacts every company, but the hardest hit might be those that hold and procedure massive quantities of consumer information: technology corporations, entrepreneurs, and the data brokers who join them. Even complying with the basic necessities for data access and deletion offers a large burden for a few organizations, which may not formerly have had gear for collating all of the records they keep on an individual.

However the biggest effect might be on firms who e commerce enterprise models depend upon obtaining and exploiting customer statistics at scale.

If agencies depend upon consent to procedure records, that consent now must be specific and knowledgeable–and renewed if the use modifications.

The changes made by tech giants due to GDPR:

The sector's largest groups have updated their sites to comply with GDPR.

1. FB launched a number of tools to "placed human beings in greater manipulate over their non-public regulations", through unifying its privacy options and building an "access your information" tool to allow users discover, down load and delete unique statistics on the internet site on line. The agency also pressured everyone to comply with new phrases of carrier.

2. Apple determined out a private dashboard of its non-public – no matter the fact that the employer proudly mentioned that, in contrast to its opposition, it does not accumulate heaps personal information within the first vicinity and did no longer need to exchange an awful lot to comply.

3.Google took a unique track, quietly updating products and privacy guidelines without drawing interest to the changes.

Influence of GDPR on business models

Companions will immediately face fines for breaches of the GDPR, even as in the past they might face best claims from their counter-events. This can put even more pressure on partners to be compliant and could create a blocker for start-united states of America and small agencies that might not be able to come up with the money for the cost of compliance.

Businesses counting on offerings events will be seeking a certification of compliance from their partners. Given the size of the potential fines, even a bank guarantee or legal responsibility waiver may not be sufficient.

Influence of GDPR on organizations

1. Expanded Jurisdiction and Scope

2. Stricter Requirements for Consent

3. More Practical and User-Friendly Privacy Policies

4. Restrictions on Direct Marketing and Profiling

5. Removal of Notification Requirement, Imposition of Documentation and Accountability

6. The Principle of "Privacy by Design"

7. Increased Data Security

8. Appointment of a Data Protection Officer

Organizations will need to update regulations and approaches in order to reflect GDPR necessities, which include how organizations obtain and use consent and also how they keep facts.Data Protection Impact Assessments (DPIA) will need to be conducted, to design data privacy into any new systems and processes. Those tests are in particular critical for any new technologies that use large-scale processing of special statistics categories, or any profiling that can affect individuals.

Influence of GDPR on Individuals:

1. The principle GDPR-related rights for citizens to preserve in mind are Breach Notification, proper to access, right to be forgotten, records Portability and privacy by design. It is able to be argued that the right to get admission to and the right to be forgotten are the strongest modifications.

2. If individuals start to take gain of GDPR in huge numbers, by means of withholding consent for positive uses of records, soliciting to get entry to their non public statistics from records agents, or deleting their information from web sites altogether, it may have a seismic affect at the enterprise records.

One of the big drawbacks of GDPR compliance is of path the price to attain it. So one can grow to be compliant, it's now not enough for groups to update their internal rules. Relying on the amount of European residents' records that they process, they ought to hire a records safety Officer and make certain that their products all take a privacy first method of their very design.

This itself implies extra cyber safety functions that need to be protected in software program architecture, that means greater paintings for developers. software that gives statistics Loss Prevention or data class functions should be implemented device-wide for a better perception and manipulate of who is processing records in which. All of this, of route, comes at a value.

some other most important concern are the massive fines which groups located to be non-compliant with the center concepts of the GDPR can incur. Corporations can be fined up to €20 million or 4% of world annual turnover for the previous financial 12 months, whichever is greater, in case of non-compliance.

- The GDPR is supposed to defend people within the EU while their non-public statistics is controlled with the aid of firms outdoor the EU, however it could no longer. Weaknesses in the wording of the regulation give the threat for organizations to accumulate records and ignore the GDPR. Once statistics escapes from the GDPR, it may be handed directly to others without criminal protection.

- Even if data is amassed and processed legally below the GDPR, it could be transferred to others after which escape the protection of the law.

- If organizations reap statistics indirectly, in maximum cases it should nonetheless be situation to the GDPR. But, the application of the regulation in these cases may be simplest theoretical, in particular in the case of statistics chains.

- Non-public records is any records related to a dwelling man or woman. The GDPR offers responsibilities to processors of the records and it offers rights to people. But, even if the statistics remains personal, customers might also lose some of rights. Companies can take gain of this.

- it is able to seem reasonable that businesses must be able to method non-public data in the event that they have an excellent cause to achieve this, after thinking about the interests of the people involved. However, the way this will work in practice means that many organizations could see it as a loophole in the law.

Similar laws in other countries and comparison.

The law applies to:

1. 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
2. A company established outside the EU offering goods/services (paid or for free) or monitoring the behavior of individuals in the EU.

If the company is a small and medium-sized enterprise ('SME') that processes personal data as described above you have to comply with the GDPR. However, if processing personal data isn't a core part of your business and your activity doesn't create risks for individuals, then some obligations of the GDPR will not apply to you (for example the appointment of a Data Protection Officer ('DPO')). Note that 'core activities' should include activities where the processing of data forms an inextricable part of the controller's or processor's activities.

When the regulation applies:

Your company is a small, tertiary education company operating online with an establishment based outside the EU. It targets mainly Spanish and Portuguese language universities in the EU. It offers free advice on a number of university courses and students require a username and a

password to access your online material. Your company provides the said username and password once the students fill out an enrolment form.

When the regulation does not apply:

Your company is service provider based outside the EU. It provides services to customers outside the EU. Its clients can use its services when they travel to other countries, including within the EU. Provided your company doesn't specifically target its services at individuals in the EU, it is not subject to the rules of the GDPR.

What Countries are affected by the GDPR is a common GDPR question. The General Data Protection Regulation (GDPR) is a European Union (EU) Regulation that was accepted on April 27, 2016. The GDPR will come into force on May 25, 2018. While it is a piece of EU legislation, institutions located outside of the EU must be aware of its implications and be on their guard to avoid violating it. The physical location of the organization does not exempt or shield it from facing the consequences of non-compliance.

Institutions with offices in an EU country or that collect, process or store the personal data of anyone located within an EU country are required to comply with the GDPR. As businesses and other organizations often have an international focus and reach, it is quite probable your entity will be required to comply with the GDPR – especially if it is an entity that operates or offers services via the Internet.

Main Countries Affected by the GDPR

As mentioned above, the physical location of the institution, organization or business is not as important in determining the need to comply with the GDPR as the physical location of the data subject – the individual whose data is being collected, processed or stored. We have stated already that most organizations will find themselves subject to or impacted by the GDPR. Having said that, organizations located within the EU will likely see their practices change to a greater extent. Logically, they are more likely to process a larger amount of data belonging to individuals located in the EU. Organizations in the following countries, the EU member states, will probably be most affected by the GDPR are Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary,

Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.

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

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

GDPR Affect on Non-EU Nations

The GDPR will have a global impact even with the relatively small and localized nature of the EU itself. Despite EU countries being more likely to see the most change, non-EU countries are likely to see greater disruption following the introduction of the GDPR. This is due to the fact that organizations located within the EU are more likely to be prepared for the changes as they as more likely to be aware of the introduction of the GDPR. A large number of organizations located outside of the EU are still unaware of the coming change or are of the opinion that they are exempt or will be unaffected. There is also a sociological difference at play: non-EU societies such as the United States (US) and others do not have the same expectation of privacy as many EU societies. Privacy laws are in place for certain types of "sensitive" data, such as the Health Insurance Portability and Accountability Act (HIPAA), which regulates healthcare information; or the Gramm-Leach-Bliley Act, which concerns financial information; but "general" data does not enjoy the same protections. For this reason, only US-based organizations and businesses that have Privacy Shield certification will be able to migrate data from the EU.

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

Transferring Data Outside of the EU

The GDPR places strict controls on data transferred to non-EU countries or international organizations.

Data is allowed to be transferred only when the EU Commission has deemed that the transfer destination “ensures an adequate level of protection”.

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

– Commission approved data protection clauses

– Legally binding agreements between public authorities

– Commission approved certification

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

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

Technological impact of GDPR

Impact of GDPR on IOT

IOT:

The GDPR applies to each non-public records and personal touchy facts, and it's far therefore critical that the ones involved within the net of things (IOT) subject be aware of the implications that the new information guidelines can have upon IOT gadgets, systems and packages. it is worth noting of route that personal information doesn't contact all IOT packages, especially in regards to the IOT (commercial net of things), and so GDPR is not a challenge for all.

IOT devices and structures which keep non-public information ought to include a patron tool, which include a smart watch, or an organization utility, which includes linked clinical system. Any security breach of such need is to be said right now. A security breach is classified as such whilst the breach is in all likelihood to bring about a chance to the rights and freedoms of people, as an instance the records has been accessed by an unauthorized source. Safety breaches need to be stated to the applicable supervisory authority within seventy two hours of the agency turning into aware of it, or the enterprise could face GDPR fines.

Taking impact in May additionally 2018, GDPR will set new standards for internet of things statistics collection and processing inside the European Union, and will introduce a unified set of policies for corporations coping with person records. This puts sure duties on tool producers and software program companies, as they may need to tailor their strategies for that reason in order to comply with the brand new policies.

Understand the GDPR requirements

A common place mistake is questioning that the GDPR has nothing to do with you or gained impact your commercial enterprise at once. Even in case you are located outside of the EU, you still have to make sure your merchandise follow the local rules to be able to avoid fines and felony problems in the destiny. As an example, it may be hard to control wherein the IOT product is used, even if you have initially constructed it with a focus on a certain United States of America. A common place mistake is wondering that the GDPR has nothing to do with anyone

or gained effect of their commercial enterprise immediately. Even in case they are positioned out of doors of the European, They must make sure their merchandise follow the local law with a purpose to keep away from fines and legal issues in the destiny.

For example, it may be tough to manipulate wherein your IoT product is used, even if you have initially built it with a focus on a certain country. As a consequence, you want to remember the fact that a number of your devices or software might become within the EU.

Broaden a solid mitigation method

One extra vital factor of the new law that every IoT enterprise wishes to consider is the importance of an incident reaction plan. In line with the GDPR, each the customers and authorities need to be notified of any records breach or security violation inside 72 hours. As IoT gadgets are considered a smooth goal for hackers, having a clear mitigation approach in case of an attack is a need to.

Prioritize transparency and users' consent

Below the GDPR, you are required to get the customers' clean consent for data series and processing. The sorts of amassed records and its reason must be in reality stated inside the consent request. Plus, users have the proper to withdraw their consent at any time.

To comply with the GDPR you need to place transparency and users' hobbies primarily. In truth, which means consumer consent cannot receive through acceptance of the primary terms and situations listed by using default within the privacy rules. Consumer consent given with a pre-ticked container at the sign-up web page received be taken into consideration legitimate.

This is why they might possibly need to review and remodel your sign-up method and update your phrases and situations page. In addition, the GDPR presents the proper to switch consumer statistics among providers or completely erase their statistics from the vendor's database on request. All of those requirements should be constructed into your device by way of default and be made easily handy for your customers.

Keep in mind the restrictions and be geared up to adapt

Additional implications concerning the net of things privacy problems are tied to the IoT products targeting youngsters. Children elderly 13 and older can now provide consent to proportion their facts beneath the GDPR. However, for youngsters aged thirteen-15, this may depend upon the unique rules in each member country (although it is now allowed through default in maximum European states). A number of the elements of the new regulation might be elaborate, but it doesn't mean you may ignore them.

Put professionals in price of facts safety

As the industry matures, there could be greater changes to come in the IoT information security sphere. To put together for the new demanding situations, it's miles vital to lease a devoted DPO.

Technological impact of IOT on GDPR:

With the upward thrust of the IoT and associated technologies consisting of robotics, AI and large facts, new regulatory frameworks are deployed in an age wherein data is gold. Moreover, the Internet of factors desires particular attention inside the scope of, among others, the GDPR and the e-Privacy regulation.

In May 2018, the EU preferred information protection regulation, also referred to as GDPR, will become enforceable. This regulation has some distance-reaching effects. The GDPR fines in case of records breaches or non-compliance may be very excessive. as the GDPR is about records privacy and the protection of private information, it's clean that you must also have a look at it if you have a web of factors challenge whereby personal records is worried. The law worries all corporations that procedure personal data of European citizens, irrespective of where these organizations or 'statistics processors' are. So, it additionally applies for businesses out of EU.

ePrivacy regulation:

This regulation concerns all digital communications. The European Parliament has accepted the textual content and now it's as much as member states to take their positions. While many human beings speak approximately the ePrivacy law from the angle of the Internet (cookies), e-mail and different digital communications channels which we all recognize, we

formerly talked about that the ePrivacy law text additionally surely mentions new electronic communication channels. These encompass on the spot Messaging apps and tools like Snap Chat and Face book Messenger. But it additionally and absolutely mention for the Internet of things. As we wrote earlier than, “the precept of confidentiality have to observe to cutting-edge and future method of communication”. And this includes the Internet of factors.

AI

GDPR will surely have an impact at the improvement and use of AI technology. corporations challenge to the European regulation will want to get explicit permission from users when they are seeking for to acquire, method, shop, transfer, or in any other case use their records — and statistics is what AI wishes to study.

Plenty of AI structures run into the “black container” problem, in that they’re not very obvious about how their system mastering algorithms attain choices. For clients, this means you don’t always understand why AI might also suggest what it recommends or take the actions it takes.

There’s absolute confidence the black container trouble becomes troublesome the greater AI is followed in advertising and marketing and other industries. at some point, marketers will want a few concept of the way systems make selections, specifically as these structures propose more state-of-the-art advertising and marketing moves.

And the more information available for device getting to know, there might be higher a device's prediction. As artificial intelligence is constructed on droves and droves of records, groups that make use of AI could have brought barrier to deploying this technology. With recognize to processing that has direct prison outcomes on the patron, together with credit score packages, e-recruiting or workplace tracking, the GDPR will restrict the usefulness of AI for these purposes

Establishment of new special categories of data

This is one of the innovations of the GDPR

Influence of GDPR on Health care centers will fall under this category.

Health care centers should have GDPR compliance because the health data of an individual should be confidential. The health data may contain personal information like

- Genetic information or information related to mental health. This data is used in the identification a person. Those genetic characters may reveal the person's unique identity. So there is a need for protecting such data.
- Physiological data which is related to the physical health will disclose the identity of a person.
- Biometric data contains the facial features and iris and fingerprints of a person.
- Apart from the patient's health information, financial records like medical bills and payments will also be maintained by the health care centers.
- The information related to person's health insurance policies will also be maintained by the health care centers.

There is a need in protecting this data because they may reveal the identity and the personal information of a specific individual.

The protection of such data also requires some obligations and duties.

- According to "right to be forgotten" the health care centers should create a system which will accept and reject all the requests and the individuals can exercise all their rights.
- The health care centers should take care of installing new software and introducing new policies.
- The processing should be done for the equipments used for medical purposes as they contain personal information about the person.
- Connected hospitals should have supply chain compromise and consent to reveal patient's data.

Impact of GDPR on supply chain management:

In supply chain management, each company will be working with a new supplier. In this case the data should be secured as it will be transferred between the suppliers and the vendors. There is also a need to know what data should be should be transferred and how long should it be kept transparent.

GDPR permeates all levels of an organization and its supply chain, and it brings into play personal data management within supply chains very quickly. GDPR impacts specific measures such as data encryption within purchased services to ensure security, confidentiality, integrity,

morality and resilience of data. According to experts, some key factors that companies need to consider to ensure that their supply chains are GDPR compliant includes creating mechanism to structure data, audits to understand where data is held, protocols to react to situations such as "right to be forgotten" requests, and regular data and privacy audits.

The good news it that there are several new tools and platforms for vendor management that factor in GDPR compliance into their frameworks, reducing risk for companies, particularly smaller ones that may lack the resources to conduct detailed audits or even provide guidelines to all of their suppliers. But to truly succeed in this environment, it is believed that companies need to make data privacy part of their corporate culture.

3. RESULTS AND DISCUSSIONS

STATISTICS	STATISTICS SOURCE
Fifty-nine percent of brand respondents and 40% of agency respondents said that their organizations have either appointed or are planning to appoint a data protection officer.	**ENCONSULTANCY**
Sixty percent of respondents said GDPR has significantly changed their organizations' workflows for collecting, using, and protecting personal information.	**MCDERMOTT, WILL & EMERY**
Marketers who were asked about their top three priorities ahead of the legislation's enforcement cited reviewing their consent mechanisms for collecting and processing data (86% of brand marketers and 77% of agency-side respondents	**ENCONSULTANCY**

Future of GDPR:

On May additionally 25, 2018, the door to the brand new regulatory era opened and we had gone through the general statistics safety regulation (GDPR) threshold.

According to the revised legal guidelines to defend and empower European citizens' facts privacy, clients can take possession and manipulate of ways their personal facts is used and shared.

Until now, GDPR discussions have largely targeted on compliance requirements. But for the ones within the coverage enterprise who're visionary and strategic, that is a lot extra than a regulatory nuisance; it will open the door to modern new business fashions for the destiny. Forward questioning firms ought to look to take advantage of the new law to provide purchasers betterofferings and studies, without jeopardizing data safety and privacy.
For people who choose to no longer appearance beforehand and content themselves with absolutely complying with GDPR, the risks of being left in the back of are very real. it's far probable they will be sidelined with the aid of bold contenders – incumbents and new entrants alike - which can be willing enough to include alternate and are geared up to build exactly the kind business they need. The GDPR door is commencing, and for the ambitious, the rewards are there for the taking.

4. CONCLUSION:

GDPR compliance is not a problem to be taken lightly, as we've mentioned within the contents of this text no longer simplest does it impose harsh fines on corporations which neglect person's personal information protection and privacy, it additionally poses serious dangers in phrases of enterprise photograph, affects enterprise's competitiveness available on the market and the general best of services it provides.

But, corporations must now not have a look at this regulation as a stipulation, but as an alternative as a possibility to benefit an advantage over competitors inside the future absolutely-regulated marketplace, build on consumer loyalty and trust, and enhance their facts control structures. The overall information protection law is a huge step to the intense future of the current personal data market.

5. REFERENCES:

- Skendžić, A., Kovačić, B., & Tijan, E. (2018, May). General data protection regulation—Protection of personal data in an organisation. In *2018 41st International Convention on*

Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1370-1375). IEEE.

- Tesfay, W. B., Hofmann, P., Nakamura, T., Kiyomoto, S., & Serna, J. (2018, March). PrivacyGuide: towards an implementation of the EU GDPR on internet privacy policy evaluation. In *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics* (pp. 15-21). ACM.
- Bourgeois, J., Kortuem, G., & Kawsar, F. (2018, October). Trusted and GDPR-compliant research with the internet of things. In *Proceedings of the 8th International Conference on the Internet of Things* (p. 13). ACM.
- Lopes, I. M., & Oliveira, P. (2018, June). Implementation of the general data protection regulation: A survey in health clinics. In *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE.
- Russo, B., Valle, L., Bonzagni, G., Locatello, D., Pancaldi, M., & Tosi, D. (2018). Cloud Computing and the New EU General Data Protection Regulation. *IEEE Cloud Computing*, *5*(6), 58-68.
- Altorbaq, A., Blix, F., & Sörman, S. (2017, December). Data subject rights in the cloud: A grounded study on data protection assurance in the light of GDPR. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 305-310). IEEE.
- Pantlin, N., Wiseman, C., & Everett, M. (2018). Supply chain arrangements: The ABC to GDPR compliance—A spotlight on emerging market practice in supplier contracts in light of the GDPR. *Computer Law & Security Review*, *34*(4), 881-885.
- Sanchez-Reillo, R., Ortega-Fernandez, I., Ponce-Hernandez, W., & Quiros-Sandoval, H. C. (2019). How to implement EU data protection regulation for R&D in biometrics. *Computer Standards & Interfaces*, *61*, 89-96.
- Gerl, A., & Pohl, D. (2018, August). Critical Analysis of LPL according to Articles 12-14 of the GDPR. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (p. 26). ACM.
- Geko, M., & Tjoa, S. (2018, November). An Ontology Capturing the Interdependence of the General Data Protection Regulation (GDPR) and Information Security. In *Proceedings of the Central European Cybersecurity Conference 2018* (p. 19). ACM.