28% overall similarity

quetext

Title: A comparative overview of data protection in e-commerce .docx

Date: 05/15/2022

Report ID: 92d1196e968531a456ca

Match #1 67% similar

Keywords: GDPR, Data protection, e-commerce, USA legislation, Republic of North Macedonia, AlbaniaINTRODUCTIONPrivacy is defined as ability of an individual or group to seclude themselves or information about themselves and thus express themselves selectively is referred to as privacy

https://en.wikipedia.org/wiki/Privacy

... For other uses, see **Privacy** (disambiguation). **Privacy** (UK: /ˈprɪvəsiː/, US: /ˈpraɪ-/)[1][2] **is** the **ability of an individual or group to seclude themselves or information about themselves, and** thereby **express themselves selectively.** When something **is** private **to** usually means that something is inherently special or sensitive to them. The domain of privacy partially overlaps with security, which can include the concepts of appropriate use and protection of information. Privacy may also take the form of bodily integrity. The right not to be subjected to unsanctioned invasions of...

Match #2 85% similar

The domain of privacy partially overlaps with the domain of security, which can include concepts such as appropriate use and information privacy and protection

https://en.wikipedia.org/wiki/Privacy

...For other uses, see Privacy (disambiguation). Privacy (UK: /ˈprɪvəsiː/, US: /ˈpraɪ-/)[1][2] is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively. When something is private to a person, it usually means that something is inherently special or sensitive to them. **The domain of privacy partially overlaps with security, which can include the concepts of appropriate use and protection of information. Privacy** may also take **the** form **of** The right not to be subjected to unsanctioned invasions of privacy by the government, corporations, or individuals is part of many countries' privacy laws, and in some cases, constitutions. The concept of universal individual privacy is a modern concept primarily associated with Western culture, particularly British and North American,...

Match #3 89% similar

The right not to be subjected to unlawful invasions of privacy by the government, corporations, or individuals is enshrined in many countries' privacy laws and, in some cases, constitutions

https://en.wikipedia.org/wiki/Privacy

...themselves selectively. When something is private to a person, it usually means that something is inherently special or sensitive to them. The domain of privacy partially overlaps with security, which can include the concepts of appropriate use and protection of information. Privacy may also take the form of bodily integrity. **The right not to be subjected to** unsanctioned **invasions of privacy by the government, corporations, or individuals is** part **of many countries' privacy laws, and in some cases, constitutions. The** concept of universal individual privacy is a modern concept primarily associated with Western culture, particularly British and North American, and remained virtually unknown in some cultures until recent times. Now, most cultures recognize the ability of individuals to withhold certain parts of personal information from wider society. With the rise...

Match #4 69% similar

While the right to privacy and the right to personal data protection are both fundamental rights enshrined in Article 8 of the EU Charter of Human Rights, they are regulated differently in different countries around the world

http://web.archive.org/web/20210423090726/https://pdpecho.c...

...things due to their wide material scope of application which could potentially cover all data related to connected devices. Protecting the fundamental right to confidentiality With the proposal for an ePrivacy regulation distinct from the GDPR, the EU makes it clear that the two sets of rules correspond to **different fundamental rights: The** GDPR is primarily an expression **of the fundamental right to the protection of personal data** as **enshrined in Article 8 of the EU Charter of Fundamental Rights, while the** ePrivacy draft regulation details **the right to** respect for private life, as **enshrined in Article** 7 **of the Charter** (see Recital 1 of the proposal). This differentiation is of great consequence, affecting the manner in which EU courts will interpret and apply the rules. The protection of the right to private life is construed so as to restrict interferences to the private life to the minimum, whereas the right...

Match #5 67% similar

With the advancement of technology and the Internet, e-commerce has undoubtedly grown drastically

http://web.archive.org/web/20200728092432/http://fordhamla...

...& Events Contact Tell the Smart House to Mind Its Own Busines s!: Maintaining Privacy and Security in the Era of Smart Devices By Kathryn McMahon Abstract Consumers want convenience. Th at convenience often comes in the form of everyday smart devic es that connect to the internet and assist with daily tasks. **With t he advancement of technology and the "Internet of** more t han ever before. Not only do consumers want convenience, they want to trust that their product is performing the task that they p urchased it for and not exposing them to danger or risk. However , due to the increasing capabilities and capacities of smart devic es, consumers are less likely to...

Match #6 66% similar

E-commerce development was, of course, faster in countries with higher levels of economic development

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3931431

...firms from 73 emerging economies on four continents were an alyzed to examine how a firm's marketing capabilities affect its p erformance. The results show that the relationship is systematica lly moderated by the level of institutional development in an em erging market. Economic conditions, legislative institutions and s ocial values all have an impact. a stronger performance impact **i n countries with higher levels of economic development** in individualistic societies. These capabilities have a weaker impact in countries with strong legislative systems Keywords: marketing capabilities, performance, institutions, economic growth, legislati ve systems, individualism emerging economies Suggested Citati on: Suggested Citation Wu, Jie and Wu, Jie, Marketing Capabilities , Institutional Development, and the Performance of Emerging M arket Firms: A Multinational Study...

Match #7 71% similar

E-commerce has many advantages of which the most important are the convenience and the global choice of goods and services and it is considered that its growth whereas increasingly appropriate for sellers and customers alike

https://core.ac.uk/download/pdf/288375411.pdf

...protection in the developing country and then evaluating the a pproaches' dispute resolution, enforcement and compliance moni toring processes for their applicability in the case of Nigeria. Ben chmarks developed by the Australian government for Industry-B ased Customer Dispute Resolution Schemes provide a suitable m echanism for evaluation. Keywords-E-commerce; Data protection ; Regulation; Nigeria; 1. **E commerce has many advantages o f which the most important are the convenience and the g lobal choice of goods and services and** can exerted an **incre asingly important** impact 1 brought to you by COREView meta data, citation **and** by Loughborough University Institutional Repo sitory https://core. ac. uk/display/288375411? utm_source=pdf& utm_medium=banner&utm_campaign=pdf-decoration-v1 on a c ountry's economy. However, the emergence of e-commerce can also bring about a number of legal, socio-economic and trust issu es, especially in developing nations where these issues pose sign ificant challenges to the organisation of electronic commerce [1]. Many online businesses...

Match #8 72% similar

As a result, many customers are concerned about their personal data being misused, which may reduce their trust in the website's services

https://core.ac.uk/download/pdf/288375411.pdf

...from such data, or /and other information which is in the posse ssion of, or is likely to come into the possession of, the data cont roller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in of **the** individual". **Many customers are concer ned about their personal data being** used inappropriately, an d this could **reduce customers' trust in the website's servic es** Fear about privacy and the lack of trust continue to be the big gest obstacles to the growth of online commerce. The Internet in dustry is built on trust between businesses [4]. These developme nts have forced several nations of the world to enact legislation and procedures to protect the information privacy...

Match #9 69% similar

In light of the issues surrounding privacy and the protection of personal data, many countries around the world have enacted legislation and procedures to protect their citizens' and corporations' information privacy

https://core.ac.uk/download/pdf/288375411.pdf

...many benefits to a country's economy and but **the** openness **of the** Internet has given rise misuse **of personal data.** Several **countries have enacted legislation and procedures to protect the information privacy of their citizens and corporations.** However, **many** developing **countries,** yet to enact any procedures, despite the high level of identity theft and online fraud. Different approaches to data privacy and protection are found in different countries. These can be generally categorised as the self-regulation approach, as used in the United States and the government approach, as used in the...

Match #10 69% similar

The main issues elaborated with the regulations, laws, and procedures are personal data protection principles such as: data minimization; data quality; purpose specification; use limitation; security safeguards; openness; individual participation and accountability

https://www.oii.ox.ac.uk/news-events/reports/data-protection-p...

...Century: Revising the 1980 OECD Guidelines By Fred H. Cate, Peter Cullen, Viktor Mayer-Schönberger "Big data is on the rise, enabling new forms of data use but also leading to new risks of data misuse. However, it is guidelines drawn up in 1980 by the Organisation for Economic Co-operation **and** Development (OECD) that have become **the** foundation for most national **laws** governing **data protection. The** OECD Guidelines took a comprehensive approach, covering **data** collection, **data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. The principles** laid out in the Guidelines were crafted for a simpler time when data types and use were less complex; organizations collected data from individuals, stored that data in a computer, and then made deterministic uses and decisions about the individual based on that data. Developed by an Oxford Internet Institute-led...

Match #11 96% similar

More than 20 years ago, the European Community felt a need to align data protection standards within their Member States in order to facilitate EU-internal, cross-border data transfers

https://lamintang.org/journal/index.php/ijlapp/article/download/...

...all these technologies are increasingly integrated. The form of telematics convergence is marked by the birth of new technology products that integrate the capabilities of information systems and communication systems based on computer systems arranged in a network of electronic systems, both in local, regional and global scope [1]. **More than 20 years ago, the European Community** (now **the EU) felt a need to align data protection standards within their Member States in order to facilitate EU internal, cross border data transfers.** At that time, national data protection laws provided considerably different levels of protection and could not offer legal certainty-neither for individuals nor for data controllers and processors. In 1995, the European Community therefore adopted Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on...

Match #12 93% similar

At that time, national data protection laws provided considerably different levels of protection and could not offer legal certainty – neither for individuals nor for the legal entities (data controllers and processors)

https://lamintang.org/journal/index.php/ijlapp/article/download/...

...based on computer systems arranged in a network of electronic systems, both in local, regional and global scope [1]. More than 20 years ago, the European Community (now the EU) felt a need to align data protection standards within their Member States in order to facilitate EU-internal, cross-border data transfers. **At that time, national data protection laws provided considerably different levels of protection and could not offer legal certainty neither for individuals nor for data controllers and processors.** In 1995, **the** Community therefore adopted Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (in short: the Data Protection Directive) in order to harmonise the protection...

Match #13 70% similar

In contrast to the Data Protection Directive, the GDPR directly applies to the EU Member States

https://lamintang.org/journal/index.php/ijlapp/article/download/...

...the Data Protection Directive) in order to harmonise the protect ion of fundamental rights of individuals with regard to data proce ssing activities and to ensure the free flow of personal data betw een EU Member States [2]. In 2016, the GDPR has been adopted to replace the Data Protection Directive from 1995. **In contrast to the Data Protection Directive, the** Regulation **directly ap plies to** its addressees no further implementation measures by **t he EU Member States** required. By equalising the rules for dat a protection, the GDPR shall lead to more legal certainty and rem ove potential obstacles to the free flow of personal data [2]. One issue that will have to be considered is the GDPR's "erasure" righ t. Article 17 of the GDPR demands that companies erase...

Match #14 91% similar

By equalizing the rules for data protection, the Regulation shall lead to more legal certainty and remove the potential obstacles to the free flow of personal data

https://lamintang.org/journal/index.php/ijlapp/article/download/...

...ensure the free flow of personal data between EU Member Stat es [2]. In 2016, the GDPR has been adopted to replace the Data Protection Directive from 1995. In contrast to the Data Protection Directive, the Regulation directly applies to its addressees-no fur ther implementation measures by the EU Member States require d. **By** equalising **the rules for data protection, the** GDPR **shal l lead to more legal certainty and remove potential obstac les to the free flow of personal data** issue that will have to b e considered is the GDPR's "erasure" right. Article 17 of the GDP R demands that companies erase the personal data of individual s when they request to be "forgotten". The GDPR does not define what "erasure of data" means, which suggests that, to comply wi th this requirement,...

Match #15 69% similar

So, the GDPR requires controllers and processors to implement technical safeguards tailored to the nature, scope, context, and purposes of the processing, as well as the risks to individuals' rights and freedoms of varying likelihood and severity

http://web.archive.org/web/20190429111849/http://refcco.com...

...global turnover or 20 Million for violating the core of Privacy by Design concepts. The rules will separate roles and responsibilitie s of the data controllers and processors, obligating controllers to deal only with those processors that provide "guarantees to impl ement appropriate technical and organizational measures" to co mply with regulations, data subjects' **rights. Controllers and p rocessors** are required **to "implement** appropriate **technical a nd** organizational measures" taking into account **"the** state **of t he** art **and the** costs **of** implementation" **and "the nature, sco pe, context, and purposes of the processing as well as the** risk **of varying likelihood and severity** for **the rights and fre edoms of** individuals." **Controllers and processors** to either a n approved code of conduct or an approved certification may use these tools to demonstrate compliance. Fairness and Transparen cy Organizations must always process personal data lawfully, fair ly, and in a transparent manner. Purpose Limitation Organization s can collect personal data only for specified, explicit, and legitim ate purposes. They cannot...

Match #16 71% similar

In the United States, the laws aim to provide "reasonable" safeguards to protect the security, confidentiality, and integrity of private information by utilizing sectoral data protection

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...a comprehensive written information security plan (WISP) addr essing 10 core standards, and (b) to establish and maintain a for mal information security programme that satisfies eight core req uirements, which range from encryption to information security t raining. In 2019, New York expanded its data breach notification l aw to include the express implement **and** maintain **"reasonable " safeguards to protect the security, confidentiality and in tegrity of private information.** Law§ 899-bb) identifies a serie s of administrative, technical, and physical safeguards which, if i mplemented, are deemed to satisfy New York's reasonableness s tandard under the law. Previously, New York prioritised the regula tion of certain financial institutions doing business in the state, b y setting minimum cybersecurity standards, with requirements fo r...

Match #17 81% similar

In states like Illinois is applicable a uniquely state law which imposes requirements on businesses that collect or otherwise obtain biometric information

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...physical safeguards which, if implemented, are deemed to satisfy New York's reasonableness standard under the law. Previously, New York prioritised the regulation of certain financial institutions doing business in the state, by setting minimum cybersecurity standards, with requirements for companies to perform periodic risk assessments and file annual compliance NYCRR 500). **Illinois** has **a uniquely** expansive **state law** (740 ILCS 14/), **which imposes requirements on businesses that collect or otherwise obtain biometric information.** Illinois Biometric Information Privacy Act (BIPA) is notable as, at the time of writing, it is the only state law regulating biometric data usage that allows private individuals to sue and recover damages for violations. In January 2019, the Illinois Supreme Court offered an expansive reading of the protections of...

Match #18 67% similar

In the same vein, personal information in the hands of banks, insurance companies, and other financial service providers, is ensured, as is the restriction of use of information bearing

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...of 20 comprehensive privacy bills before the legislatures of 15 different states. 1. 3 Is there any sector-specific legislation that impacts data protection? Key sector-specific laws include those covering financial services, healthcare, telecommunications, and education. The Gramm Leach Bliley Act (GLBA) (15 U. S. Code§ 6802(a) et seq.) protection **of personal information in the hands of banks, insurance companies and other companies in the financial service** industry. This statute addresses "Non Public **Personal Information**" (NPI), which includes any **information** that a **financial** service company collects from its customers in connection with the provision of its services. It imposes requirements on financial service industry companies for securing NPI, restricting disclosure and use of NPI and notifying customers when NPI is improperly exposed to unauthorised persons. The Fair Credit Reporting Act (FCRA), as amended...

Match #19 78% similar

on an individual's creditworthiness, credit standing, credit capacity, personal characteristic or mode of living to determine eligibility for credit, employment, or insurance, information relating to health status, provision of health

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...securing NPI, restricting disclosure and use of NPI and notifying customers when NPI is improperly exposed to unauthorised persons. The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (FACTA) (15 U. S. Code§ 1681), restricts use of information with a bearing **on an individual's creditworthiness, credit standing, credit capacity,** character, general reputation, **personal** characteristics **or mode of living to determine eligibility for credit, employment or insurance.** It also requires the truncation **of credit** card numbers **on** the secure destruction of certain types of personal information, and regulates the use of certain types of information received from affiliated companies for marketing purposes. In addition to financial industry laws and regulation, the major credit card companies require businesses that process, store or transmit payment card data to comply...

Match #20 73% similar

METHODOLOGYDue to various reasons, different approaches to data privacy and protection are found in the United States and the European Union, the self-regulation and government regulation approach respectively

https://www.researchgate.net/publication/307624884_Privacy_...

...set up a framework which incorporates the environmental context, ethical perspectives and firm-specific considerations to help firms develop a strategy for handling digital privacy concerns. Data privacy approaches from US and EU perspectivesArticleMay 2002 Gerhard SteinkeConsumers using the Internet often indicate that the privacy of their personal data is concern with **the** new technology. **Different approaches to data privacy and protection are found in the United States and the European Union** an emphasis on **self regulation in the** former versus strict legal requirements **in the** The implications of the recent "safe harbor" agreement may have a significant impact on privacy expectations in the US. Values, personal information privacy, and regulatory approachesArticleDec 1995COMMUN ACM Sandra MilbergSandra J. BurkeH. Jeff SmithErnest A. KallmanThe relationships among nationality, cultural values, personal information privacy concerns, and information privacy regulation...

Match #21 75% similar

4 trillion US dollars in 2022. Online shopping is one of the most popular online activities worldwide

https://finance.yahoo.com/news/digital-freight-forwarding-mark...

...logistics industry is developing into a paperless digitized industry supporting the growth of the market. Key Market TrendsGrowth in E-Commerce driving Digital Freight Forwarding MarketIn 2019, retail e-commerce sales worldwide amounted to around 3. 53 trillion US dollars and e-retail revenues are projected to grow even further at a pace **in the** coming few years. **Online shopping is one of the most popular online activities worldwide,** both domestic and cross-border e-commerce is booming in developing markets such as China, India, and Indonesia due to that reason. This encompasses not just direct-to-consumer retail, but also shipments of electronics, pharmaceuticals, and consumer packaged goods. With increasing access to the internet even the manufacturers of products are gradually moving...

Match #22 92% similar

Thereby the, Article 2 of the GDPR states that "the regulation applies to the processing of personal data wholly or partly by automated means and to the processing of personal data other than by automated means that form part of a filing system or are intended to form part of a filing system

http://web.archive.org/web/20201130174405/https://www.itgov...

...anywhere in the world that processes the data of EU residents. With the Regulation expanding the definition of personal data, many organizations are uncertain what the definition now includes. The scope of personal data Let's start with the circumstances under which the processing of personal data must meet the GDPR' requirements. **Article 2 of the GDPR states that the Regulation applies to "the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data** which **form part of a filing system or are intended to form part of a filing** personal data? The GDPR's definition of personal data is broad. Article 4 states that "'personal data' means any information relating to an identified or identifiable natural person ('data subject')." It adds that: "An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to...

Match #23 60% similar

" This applies to any processing of personal data and is important for businesses that deal with e-commerce

https://www.allenovery.com/global/-/media/allenovery/2_docum...

...technology and data to combat and exit from the Covid-19 coronavirus crisis, in particular concerning mobile applications and the use of anonymised mobility data (Recommendation, see further in this document). The Toolbox aims to facilitate establishment of effective, interoperable app solutions throughout the EU that are based on privacy-enhancing minimise the **processing of personal data and** support cross border situations. **To this** essential apps requirements, including the epidemiological framework, technical functionalities, cross-border interoperability requirements and cybersecurity measures and safeguards; The press release about the Toolbox is available here. The Toolbox is available here. The press release about the data protection guidance is available here. The Data Protection Guidance is available here....

Match #24 80% similar

According to the European Union's Court of Justice in the case Google Spain SL-Google Inc

http://web.archive.org/web/20210417094331/https://www.hipa...

...million) GDPR fine by the Swedish Data Protection Authority (DPA) over the failure to comply with 'right-to-be-forgotten' requests from EU citizens to have web pages removed from its search engine listings. The right to be forgotten in the EU predates GDPR. It was first introduced in EU legislation in 2014 ruling by **the Court of Justice of the European in the case, Google Spain SL, Google Inc** Española de Protección de Datos, Mario Costeja González. The law requires search engines to remove links to freely accessible webpages that appear in search results generated from a search of an individual's name, if that individual requests the listing is removed and if certain conditions are satisfied. GDPR strengthened the...

Match #25 100% similar

extent than any other jurisdiction in the world

https://www.jipitec.eu/issues/jipitec-9-2-2018/4723

...operators, but impacts the vast majority of websites that collec t the "click stream data" (surfing behaviour), [28] either through the use of cookies, ad banners or JavaScript. 29 In conclusion, Ar ticle 3(2) significantly increases the scope of EU data protection r ules in a unilateral way, and to a greater **extent than any othe r jurisdiction in the world** has done until now. Even if it refers to the alleged voluntary conduct of the operator to justify the ap plication of the regulation, in practice the application of the regul ation almost "follows" the EU data. Given the sudden application of EU rules to many websites around the world, one may...

Match #26 60% similar

This is the case for occasional processing that does not affect special categories of personal data or personal data relating to criminal convictions and offences on a large scale and is unlikely to endanger individuals' rights and freedom. All three conditions must be met concurrently

https://transparency.mk/wp-content/uploads/2022/02/fight_mo...

...to request the restriction or suppression of the processing of th eir personal data. 91 That is, to move, copy, or transfer personal data from one data controller to another safely and securely, wit hout affecting its usability. 50- require large scale, regular, and s ystematic monitoring of individuals (for example, **or** consist **of la rge scale processing of special categories of data or data relating to criminal convictions and offences.** 92 DPOs **mus t:** inform **and** advise **the** highest level **of** management **and** emp loyees about obligations **to** comply with **the** Law; monitor compli ance with **the** Law, **and** with **data** protection policies, including managing internal **data** protection activities, raising awareness o f data protection issues, training staff, and conducting internal a udits;- advise on, and to monitor, DPIAs;- cooperate with the DZL P; and- be the first point of contact for the DZLP and for individua ls whose data is processed (employees, customers and others). 9 3 Finally,...

Match #27 68% similar

The primary responsibility of the representative is to act as a point of contact for Supervisory Authorities in order to ensure compliance with the GDPR, to keep the controller's records of processing activities, and to be subject to enforcement proceedings in the event of non-compliance by the data controller or processor

https://www.jipitec.eu/issues/jipitec-9-2-2018/4723

...as its name implies, is to represent foreign operators with rega rd to their obligations and create a point of contact between the m and the EU authorities. More specifically, the representative is required to cooperate with the authorities regarding any action o rdered to ensure compliance with the regulation. [48] 54 Howeve r, this function **and** actually elevate **the representative as a p rimary** tool **of enforcement.** Indeed, recital 80 provides that **th e** designation **of** such **a representative** does not affect **the res ponsibility or** liability **of the** operator, but adds that **the repre sentative** "should **be subject to enforcement proceedings i n the event of non compliance by the controller or** process or". **In a** previous draft **of the** regulation, this statement was ma de under Article 27, before being displaced to the preamble of th e regulation. Unfortunately, the regulation does not provide any details on the enforcement mechanisms in question. 55 There is much controversy as to whether a representative may incur som e sort of liability, in addition to...

Match #28 60% similar

This is the GDPR's known obligation of transparency regarding the processing of personal data

http://web.archive.org/web/20220117135244/http://fox-electro...

...or cessation of processing due to fulfillment of the Processing P urpose for which the Consent was given and/ or cessation of proc essing due to decisions of the state body responsible for supervis ion over the processing of Personal Data. In all these cases, your Personal Data will be deleted If you have any questions **regardi ng the processing of the** above **Personal Data,** you would lik e to revoke this Consent for any reason and at any time, and if y ou consider it necessary to correct your Personal Data, please co ntact us in writing (by sending a registered mail, fax or e-mail) to the following address: Vimport d. o. o., Batajnički drum 23, 1100 0...

Match #29 77% similar

Transparency is about instilling trust in the processes that affect data subjects/users by allowing them to understand and, if necessary, challenge those processes; it is also an expression of the fairness principle

http://ced.revistas.deusto.es/article/download/1756/2158

...in advertising) about their use of credit history information and the impact that it can have on their decisions. In the European U nion, and specifically in the context of the General Data Protectio n Regulation (from now on, GDPR)23, the requirement for transp arency is of particular importance. As the EDPB /WP2924 **«it is a bout** engendering **trust in the processes** which **affect the** citi zen **by** enabling **them to understand, and if necessary, chall enge those processes. It is also an expression of the princ iple of fairness in** relation **to the** of personal data expressed in Article 8 of the Charter of Fundamental Rights of the European U nion»25. The GDPR regulates the principle of transparency in Arti cle 5 (a) -in accordance with Recital 39- and develops it in Article 12, which applies transversally to information, communications a nd modalities of exercise relating...

Match #30 79% similar

Regarding the records of data, it must include, among other things, information on the purposes of processing, the types of data affected, and a description of the technical and organizational security measures used

https://www.scribd.com/book/375385348/Data-Protection-Officer

...into compliance with the GDPR. Different organizational require ments will have to be fulfilled. Records of Processing Activities Co ntrollers and processors will have to implement records of their p rocessing activities that will-if thoroughly maintained-permit to p rove compliance with the GDPR towards the Supervisory Authorit ies and help to fulfil the information towards **the data** subjects. **Records must** contain, inter alia, **information on the purpose s of processing, the** categories **of data** that are **affected and a description of the technical and organizational security measures** TechnologyAll categoriesPublisher:Sarah TaylorReleas ed:Mar 31, 2018ISBN:9781386191209Format:BookAbout the aut horSTSarah TaylorSarah Taylor has a BA in History and an MSLS. She enjoys reading and writing about history, playing piano, and going on park walks with her dog. You may find her at https://bea utifuldreamerdotcom. wordpress. com and Goodreads at https:// www. goodreads. com/author/show/21550493. Sarah_Taylor. Rea d...

Match #31 61% similar

In some cases, if the intended processing activity, particularly the use of new technologies, is likely to result in a high risk to data subjects' rights and freedoms, the entities planning or dealing with e-commerce must conduct a preventive Data Protection Impact Assessment

https://transparency.mk/wp-content/uploads/2022/02/fight_mo...

...re-access and availability in case of physical or technical disrup tion; and• regular testing, assessment and evaluation of processi ng safety measures. Not later than 72 hours after having becom e aware of a personal data breach, the controller is obliged to no tify the Agency, unless the personal data breach is **to result in a risk to the rights and freedoms of** natural persons. Privacy **impact assessment** (PIA): **If some** type **of processing is likel y to result in a high risk to the rights and freedoms of** natu ral persons, **in** particular due **to the use of new technologies and** taking into account **the** nature, scope, circumstances **and** p urpose **of processing,** before starting **the processing the** cont roller will assess its **impact** data protection. The Law further spe cifies cases in which an impact assessment is required. These inc lude large-scale systematic surveillance in public areas, and syst ematic and comprehensive assessment of the status and charact eristics of a natural person with the aid of automated processing, including profiling, etc. Under the previously adopted law...

Match #32 77% similar

" Furthermore, based on Article 12 of the GDPR it is thought that clear and plain language fulfills the requirement because information should be provided in as simple a manner as possible, avoiding complex sentence and language structures

http://web.archive.org/web/20211225144743/https://gdprhub.e...

...by way of contextual pop-ups which activate when a data subje ct fills in an online form, in an interactive digital context through a chatbot interface, etc). Clear and Plain Language[edit edit sour ce] With written information (and where information is delivered orally, or by audio/ audiovisual methods, including for vision-imp aired for **clear** communication **should be** followed. **The require ment** for **clear and plain language** means **that information should be provided in as simple a manner as possible, avo iding complex sentence and language structures. The info rmation should be** and definitive; it should not be phrased in a bstract or ambivalent terms or leave room for different interpreta tions. In particular, the purposes of, and legal basis for, processin g the personal data should be clear. Language qualifiers such as "may", "might", "some", "often" and "possible" should also be av oided. Where data...

Match #33 85% similar

The information should be concrete and definitive; it should not be phrased in abstract or ambiguous terms, nor should it leave room for multiple interpretations

http://web.archive.org/web/20210511020057/https://www.lexol...

...recommends written notification. The data controller should de cide on the appropriate form of notification, taking into account a ll the circumstances of each particular case. Language The requir ement for clear, plain language means that information should b e provided in as simple a manner as possible, avoiding complex sentences and language structures. **The information should b e concrete and definitive; it should not be phrased in abst ract or** ambivalent **terms or leave room for** different **interpre tations.** a few examples of 'do's' and 'don'ts'. Accessibility The ' easily accessible' requirement means that the data subject shoul d not have to seek out the information. WP29 recommends that t he data controller should ensure that it is immediately apparent where this information can be accessed, for example by providin g it directly...

Match #34 98% similar

The GDPR introduces a general reporting duty of the controller towards the Supervisory Authorities in case of personal data breach

http://cdsutherland.blogspot.com/2018/03/general-data-protec...

...processors. Organizations will have to proactively fulfill many o bligations towards the data subjects, such as granting informatio n on processing, erasing personal data or rectifying incomplete p ersonal data. Especially, the data subjects' right to data portabilit y may challenge entities as they will have to provide datasets to their customers upon request. **The GDPR introduces a genera l reporting duty of the controller towards the Supervisory Authorities in case of a personal data breach.** Such breach might occur by way of a technical or physical incident. The notifi cation has to take place within a 72-hour time frame after becom ing aware of the breach. In case of an incident with a high risk fo r the rights and freedoms of the data subjects concerned, the...

Match #35 100% similar

Such breach might occur by way of a technical or physical incident

http://cdsutherland.blogspot.com/2018/03/general-data-protec...

...data or rectifying incomplete personal data. Especially, the dat a subjects' right to data portability may challenge entities as the y will have to provide datasets to their customers upon request. The GDPR introduces a general reporting duty of the controller to wards the Supervisory Authorities in case of a personal data brea ch. **Such breach might occur by way of a technical or physi cal incident.** The notification has to take place within a 72-hour time frame after becoming aware of the breach. In case of an inc ident with a high risk for the rights and freedoms of the data subj ects concerned, the controller will have to communicate the brea ch also to them. In such...

Match #36 95% similar

The notification has to take place within 72-hous time frame after becoming aware of the breach

http://cdsutherland.blogspot.com/2018/03/general-data-protec...

...data portability may challenge entities as they will have to pro vide datasets to their customers upon request. The GDPR introdu ces a general reporting duty of the controller towards the Superv isory Authorities in case of a personal data breach. Such breach might occur by way of a technical or physical incident. **The notif ication has to take place within** a 72-hour **time frame after becoming aware of the breach.** In case of an incident with a h igh risk for the rights and freedoms of the data subjects concern ed, the controller will have to communicate the breach also to th em. In such a case, assistance from the Supervisory Authority wil l be available to the controller. Where feasible based on...

Match #37 95% similar

In a case of an incident with high risk for the rights and freedoms of data subjects concerned, the controller will have to communicate the breach also to them

http://cdsutherland.blogspot.com/2018/03/general-data-protec...

...The GDPR introduces a general reporting duty of the controller towards the Supervisory Authorities in case of a personal data br each. Such breach might occur by way of a technical or physical i ncident. The notification has to take place within a 72-hour time f rame after becoming aware of the breach. **In case of an incide nt with a high risk for the rights and freedoms of the data subjects concerned, the controller will have to communica te the breach also to them.** In such a case, assistance from th e Supervisory Authority will be available to the controller. Where feasible based on an entity's budget and resources, compliance with the GDPR might be implemented and monitored by way of a Data Protection Management System. It is an internal complianc e system that will monitor...

Match #38 62% similar

Data protection regulations for e-commerce in the United States of AmericaAs stated in Section 2, there is no unified legal system for the protection of personal data in the United States of America

http://web.archive.org/web/20201221130423/https://www.licksl...

...ProtectionCorporate& TransactionsArbitrationSectorsMedia& EntertainmentLife SciencesTelecom& IoTInfrastructureDefenseSectorsMedia& EntertainmentLife SciencesTelecom& IoTInfrastructureDefenseOur TeamEVENTSNews& EVENTSNewseventsPublicationsClient AlertHANDOUTSGAIR BLOGPPH GraphicsPdp GraphicsBRPTO Documents& Charts ExaminationGuidelinesProsecutionCharts BLOGBLOGComplianceGovernment Affairs &International RelationsCONTACTContact usContact uswORK WITH USintranetclientsLicks Attorneys' Government Affairs& International Relations BlogDoing Business in Brazil: Political and economic landscapeLicks Attorneys' COMPLIANCE BlogAnd how about **the** privacy and **protection of personal data in the United States of America?** December 21, 2020No items found. **In** this unique year **of** 2020, **the** significant milestone **in the** area **of** privacy and **protection of personal data in the United States of America** undoubtedly the CCPA- California Consumer Privacy Act, which started to protect the citizens of the State of California against commercial use of their personal data without their consent. But does privacy and protection of personal data in the US come down to the CCPA only? Of course not! In...

Match #39 84% similar

Also, entities established in other jurisdictions may be subject to both federal and state data protection laws for activities impacting USA residents and whose information are collected, hold, transmit, process or share

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...unauthorised access or acquisition of computerised data that compromises the security, confidentiality, or integrity of personal information. 3. Territorial Scope 3. 1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to Businesses **established in other jurisdictions may be subject to both federal and state data protection laws for activities impacting** United States **residents whose information** the business collects, holds, transmits, processes **or** Principles 4. 1 What are the key principles that apply to the processing of personal data? Transparency The FTC has issued guidelines espousing the principle of transparency, recommending that businesses: (i) provide clearer, shorter, and more standardised privacy notices that enable consumers to better comprehend privacy practices; (ii) provide reasonable...

Match #40 71% similar

Transparency, lawful basis for processing, purpose limitation, data minimization, proportionality, and retention are the key principles defined in US data protection legislation, as they are in the GDPR

https://www.pillsburylaw.com/images/content/1/1/v2/117865/D...

...and reproduced with kind permission by Global Legal Group Ltd, London U SA 4 Key Principles 4. 1 What are the key principles that apply to the processing of personal data? Transparency US data protection statutes are focused generally on security of the data. As such, the European principles **transparency, lawful basis for processing, purpose limitation, data** minimisation, **proportionality and data retention are** not addressed **in the** statutes. We note that there is guidance regarding a minimum period of time **in** like employee records, must be retained, but there is not necessarily a requirement for the destruction of those records after that time has expired. This is left to a company's decision. Lawful basis for processing This is not applicable. Purpose limitation This is not applicable. Data minimisation This is...

Match #41 81% similar

and more standardized privacy notice/policy that enable consumers to better comprehend privacy practices; Providing reasonable access to the consumer data they maintain; and Expanding efforts to educate consumers about commercial data privacy practices

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...United States residents whose information the business collects, holds, transmits, processes or shares. 4. Key Principles 4. 1 What are the key principles that apply to the processing of personal data? Transparency The FTC has issued guidelines espousing the principle of transparency, recommending that businesses: (i) provide clearer, shorter, **and more** standardised **privacy** notices **that enable consumers to better comprehend privacy practices;** (ii) provide **reasonable access to the consumer data they maintain that** is proportionate **to the** sensitivity of **the data and the** nature of its use; **and** (iii) expand **efforts to educate consumers about commercial data privacy practices.** basis for processing While there is no "lawful basis for processing" requirement under U. S. law, the FTC recommends that businesses provide notice to consumers of their data collection, use and sharing practices and obtain consent in limited circumstances where the use of consumer data is materially different than claimed...

Match #42 78% similar

Despite the fact that according to the USA legislation there is no “lawful basis for processing” requirement, the FTC recommends that entities provide notice to consumers of their data collection, use and sharing practices and should obtain consent in limited circumstances (if sensitive data is collected)

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...(i) provide clearer, shorter, and more standardised privacy noti ces that enable consumers to better comprehend privacy practic es; (ii) provide reasonable access to the consumer data they mai ntain that is proportionate to the sensitivity of the data and the n ature of its use; and (iii) expand efforts to educate consumers co mmercial **data** privacy **practices. Lawful basis for processin g** While **there is no "lawful basis for processing" requireme nt** under U. S. law, **the FTC recommends that** businesses **pro vide notice to consumers of their data collection, use and sharing practices and obtain consent in limited circumsta nces** where **the use of** consumer **data is** when the data was col lected, or where sensitive data is collected for certain purposes. Purpose limitation The FTC recommends privacy-by-design practi ces that include limiting "data collection to that which is consiste nt with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically...

Match #43 84% similar

The FTC also recommend privacy-by-design practices that include limiting data collection to that which is consistent with the context of the business

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...the FTC recommends that businesses provide notice to consum ers of their data collection, use and sharing practices and obtain consent in limited circumstances where the use of consumer dat a is materially different than claimed when the data was collecte d, or where sensitive data is collected for certain purposes. Purp ose **The FTC** recommends **privacy by design practices that i nclude limiting "data collection to that which is consistent with the context of** a particular transaction or **the** consumer's relationship with the business, or as required or specifically auth orized by law". Data minimisation See above. Proportionality See above. Retention The FTC recommends privacy-by-design practic es that implement "reasonable restrictions on the retention of da ta", including disposal "once the data has outlived the legitimate purpose for which it was collected"....

Match #44 67% similar

Appointment of a Data Protection Officer is not required under USA special laws, contrary to what is stated in the GDPR

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...concerning the typical amount of time for the data broker regis tration process. 7. Appointment of a Data Protection Officer 7. 1 I s the appointment of a Data Protection Officer mandatory or opti onal? If the appointment of a Data Protection Officer is only man datory in some circumstances, please identify those circumstanc es. **Appointment of a Data Protection Officer is not require d under** U. S. law, but certain statutes require **the appointmen t** of an individual or individuals who are charged with compliance with the privacy and data security requirements under the statut e. These include the GLBA, HIPAA, and the Massachusetts Data S ecurity Regulation, for example. 7. 2 What are the sanctions for f ailing to appoint a Data Protection Officer where required? Potent ial...

Match #45 84% similar

Certain statutes, however, require the appointment or designation of an individual or individuals who are charged with enforcing the statute's compliance and data security requirements

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...of a Data Protection Officer 7. 1 Is the appointment of a Data Pr otection Officer mandatory or optional? If the appointment of a D ata Protection Officer is only mandatory in some circumstances, please identify those circumstances. Appointment of a Data Prot ection Officer is not required under U. S. law, **certain statutes r equire the appointment or designation of an individual or individuals who are charged with compliance with the** priv acy **and data security requirements** under **the** include the GL BA, HIPAA, and the Massachusetts Data Security Regulation, for example. 7. 2 What are the sanctions for failing to appoint a Dat a Protection Officer where required? Potential sanctions are statu te/regulator-specific. 7. 3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of...

Match #46 66% similar

As a result, the specific qualifications for the Data Protection Officer, his responsibilities, registration and notification to the relevant data protection authority, and the obligation to publish the name of the Data Protection Officer in the privacy notice or equivalent document are not defined

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...not applicable in our jurisdiction. 7. 4 Can a business appoint a single Data Protection Officer to cover multiple entities? This is n ot applicable in our jurisdiction. 7. 5 Please describe any specific qualifications for the Data Protection Officer required by law. This is not applicable in our jurisdiction. 7. What **are the responsibil ities of the Data Protection Officer as** required by law **or** bes t practice? This is **not** applicable **in** our jurisdiction. 7. 7 Must **th e** appointment **of a Data Protection Officer** be registered/notif ied **to the relevant data protection** authority(ies)? This is **not** applicable **in** our jurisdiction. 7. 8 Must **the Data Protection Of ficer** be named **in a** public facing **privacy notice or equivalen t document?** This is **not** applicable **in**. Appointment of Processo rs 8. 1 If a business appoints a processor to process personal dat a on its behalf, must the business enter into any form of agreem ent with that processor? Under certain state laws and federal reg ulatory guidance, if a business shares certain categories of perso nal information with a...

Match #47 92% similar

Concerning the use of cookies, the federal Computer Fraud and Abuse Act has been used to assert legal claims against the use of cookies for behavioral advertising, where the cookies enable "deep packet" inspection of the computer on which they are placed

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...the Truth in Caller ID Act in connection with approximately 1 bil lion robocalls. Many states have their own deceptive practices st atutes, which impose additional state penalties where violations of federal statutes are deemed to be deceptive practices under t he state statute. 10. Cookies 10. 1 Please describe any legislativ e **on the use of cookies** (or similar technologies). **The federal Computer Fraud and Abuse Act has been used to assert le gal claims against the use of cookies for** behavioural **advert ising, where the cookies enable "deep packet" inspection of the computer on which they are placed.** least two states, California and Delaware, require disclosures to be made where c ookies are used to collect information about a consumer's online activities across different websites or over time. The required dis closure must include how the operator responds to so-called "do not track" signals or other similar mechanisms. In addition,...

Match #48 100% similar

At least two states California and Delaware, require disclosures to be made where cookies are used to collect information about a consumer's online activities across different websites or over time

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...Please describe any legislative restrictions on the use of cookie s (or similar technologies). The federal Computer Fraud and Abus e Act has been used to assert legal claims against the use of coo kies for behavioural advertising, where the cookies enable "deep packet" inspection of the computer on which they are placed. **At least two states, California and Delaware, require disclosu res to be made where cookies are used to collect informat ion about a consumer's online activities across different w ebsites or over time.** The required disclosure must include how the operator responds to so-called "do not track" signals or other similar mechanisms. In addition, the FTC Act and state deceptive practices acts have underpinned regulatory enforcement and pri vate class action lawsuits against companies that failed to disclo se or misrepresented their use of...

Match #49 100% similar

The required disclosure must include how the operator responds to so-called "do not track" signals or other similar mechanisms

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...of cookies for behavioural advertising, where the cookies enabl e "deep packet" inspection of the computer on which they are pl aced. At least two states, California and Delaware, require disclos ures to be made where cookies are used to collect information a bout a consumer's online activities across different websites or o ver time. **The required disclosure must include how the op erator responds to so called "do not track" signals or othe r similar mechanisms.** In addition, the FTC Act and state decep tive practices acts have underpinned regulatory enforcement an d private class action lawsuits against companies that failed to di sclose or misrepresented their use of tracking cookies. One comp any settled an action in 2012 with a payment of US$22. 5 million to the FTC,...

Match #50 85% similar

In this context, the FTC has stated that security measures for protecting personal data must be "reasonable," taking into account a number of factors such as the volume and sensitivity of data held by the entity, the size and complexity of the company's operations, and the cost of the tools available to address vulnerabilities

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...from monitoring their employees while they are engaged in pro tected union activities. 15. Data Security and Data Breach 15. 1 I s there a general obligation to ensure the security of personal da ta? If so, which entities are responsible for ensuring that data are kept secure (e. g., controllers, processors, etc.)? **In the** consume r **context, the FTC has stated that a company's data securi ty measures for protecting personal data must be** "reasona ble", **taking into account** numerous **factors, to** include **the vo lume and sensitivity of** information **the** company holds, **the si ze and complexity of the company's operations, and the c ost of the tools that** are **available to address vulnerabilitie s.** federal statutes and certain individual state statutes also impo se an obligation to ensure security of personal information. For e xample, the GLBA and HIPAA impose security requirements on fi nancial services and covered healthcare entities (and their vendo rs). Some states impose data security obligations on certain entit ies that collect, hold or transmit...

Match #51 71% similar

Certain federal laws, as well as certain state laws, impose an obligation to ensure the security of personal data

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...stated that a company's data security measures for protecting personal data must be "reasonable", taking into account numero us factors, to include the volume and sensitivity of information th e company holds, the size and complexity of the company's oper ations, and the cost of the tools that are available to address vul nerabilities. **Certain federal** statutes and **certain** individual **sta te** statutes also **impose an obligation to ensure security of personal** example, the GLBA and HIPAA impose security require ments on financial services and covered healthcare entities (and their vendors). Some states impose data security obligations on certain entities that collect, hold or transmit limited types of pers onal information. For example, the New York Department of Finan cial Services (NYDFS) adopted regulations in...

Match #52 78% similar

As we mentioned, there is no general legal requirement to report data breaches to the relevant data protection authority

https://www.pillsburylaw.com/images/content/1/1/v2/117865/D...

...statutes and certain individual state statutes impose an obligat ion to ensure security of personal information. The Federal Gram m Leach Bliley Act and HIPAA impose such requirements on finan cial services and covered health care entities. Some states impos e data security obligations on any entities that collect, hold or tra nsmit limited information. 15. 2 **Is there** a **legal requirement t o report data breaches to the relevant data protection** If s o, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under w hat circumstances the relevant data protection authority(ies) exp ects voluntary breach reporting. At the federal level, data breach notification requirements are imposed under the Privacy Act (app licable to federal...

Match #53 94% similar

Some states laws require reporting of data breaches to a state agency or attorney general under certain conditions

https://www.pillsburylaw.com/images/content/1/1/v2/117865/D...

...on a variety of issues including children's privacy, identity theft and telemarketing. State Attorneys General have, in some cases, offered resources on their websites for victims of identity theft a nd for companies suffering data security breaches. The Departm ent of Health and Human Services has issued information on co mpliance with HIPAA. **Some state** statutes **require reporting o f data breaches to a state agency or attorney general und er certain conditions.** The information to be submitted varies b y state but generally includes a description of the incident, the n umber of individuals impacted, the types of information exposed, the timing of the incident and the discovery, actions taken to pre vent future occurrences, copies of notices sent to impacted indivi duals and any...

Match #54 97% similar

The information to be submitted varies by state but generally includes a description of the incident, the number of individuals impacted, the types of data exposed, the timing of the incident and the discovery, actions taken to prevent future occurrences, copies of notices sent to impacted individuals, and any services offered to impacted individuals, such as credit monitoring

https://iclg.com/practice-areas/data-protection-laws-and-regula...

...information that is required to be disclosed in SEC Commission filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would r ender them ineffective. Some state statutes require the reportin g of data breaches to a state agency or attorney general under c ertain conditions. **The information to be submitted varies by state but generally includes a description of the incident, the number of individuals impacted, the types of informat ion exposed, the timing of the incident and the discovery, actions taken to prevent future occurrences, copies of not ices sent to impacted individuals, and any services offere d to impacted individuals, such as credit monitoring.** 15. 3 Is there a legal requirement to report data breaches to affected d ata subjects? If so, describe what details must be reported, to wh om, and within what timeframe. If no legal requirement exists, d escribe under what circumstances the relevant data protection a uthority(ies) expect(s) voluntary breach reporting. At the...

Match #55 60% similar

Legal regulations on data protection regarding e-commerce in Republic of North MacedoniaIn a Balkan perspective, the area of personal data protection in the Republic of North Macedonia is regulated for the first time by the adoption of a special Law on Personal Data Protection in 2005 ("Official Gazette of the Republic of Macedonia No

https://dijalogkoneu.mk/en/wp-content/uploads/sites/3/2021/10...

...their processing operations. Introduction This policy document provides an overview of the standards on personal data protectio n, as stipulated under the Law on Personal Data Protection ("Offi cial Gazette of RNM" no. 42/20) and the General Data Protection Regulation (GDPR), in respect to planning, creating and introduci ng eservices by institutions, standing **on the** path **of the** institut ions **in** introducing such standards. 1 PRIVACY **PROTECTION** AS I NTEGRAL PART **OF** DEVELOPING QUALITY **E** SERVICES AND TOOL S 1. Alignment **of the** national legislation **in the** field **of person al data protection** with **the** EU acquis **In the Republic of Nor th Macedonia, the** concept **of** privacy **protection** was **first** int roduced **in 2005** with **the adoption of the Law on Personal D ata Protection ("Official Gazette of** RM" **no.** 7/05).[1] **Adopti on of** this **law** confirmed the country's commitment to align nati onal legislation on personal data protection with the Directive 95 /46 of the European Parliament and of the Council on the protecti on of individuals with regard to processing of personal data and on the free movement of such data,[2] the Convention for the Pr otection of...

Match #56 67% similar

7/2005"), the provisions of which lay the foundations of the right to personal data protection in the Republic of Macedonia

https://dijalogkoneu.mk/en/wp-content/uploads/sites/3/2021/10...

...i. e. the law enters into effect on August 24th, 2021. The new L aw on Personal Data Protection is fully aligned with the General Data Protection Regulation 2016/679, accounting for partial attai nment of the strategic goal no. 1 ("Republic of Macedonia is reco gnized as country that ensures adequate level **of personal data** protection") under **the** Strategy on Implementation **of the Right to Personal Data Protection in the Republic of Macedonia** 7-2022.[6] Full attainment of this strategic goal is expected in th e upcoming period, by adopting relevant secondary legislation a nd aligning sectoral laws with the Law on Personal Data Protectio n. https://www. dzlp. mk/sites/default/files/pdf/Zakon_za_zastita_ na_licnite_podatoci_2005. pdf https://eur-lex. europa. eu/legal-co ntent/EN/TXT/? uri=celex:31995L0046 https://www. coe. int/en/w eb/conventions/full-list/-/conventions/rms/0900001680078b37 ht tps://eur-lex. europa. eu/legal-content/EN/TXT/PDF/? uri=CELEX:0 2016R0679-20160504&from=EN https://dzlp. mk/sites/default/fil es/u4/zakon_za_zastita_na_licnite_podatoci. pdf https://dzlp. mk/s ites/default/files/dzlp_strategija_mk. pdf...

Match #57 65% similar

The legal framework for personal data protection in the Republic of North Macedonia is supplemented by the ratification of the Convention for the Protection of Individuals with regard to

https://dijalogkoneu.mk/en/wp-content/uploads/sites/3/2021/10...

...as integral par t of developing qual i ty e- ser vices and tools 2 2008 Law on Ratification of the Additional Protocol to the Conven tion for the Protection of Individuals with Regard to Automated Pr ocessing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows ("Official Gazette **of the Republic of M acedonia"** no. 103/08) 2016 General **Data Protection** Regulati on 2016/679 2020 Law on **Personal Data Protection** ("Official Gazette **of** RNM" no. 42/20) 2005 Law on **Ratification of the Co nvention for the Protection of Individuals with Regard to** A utomatic Processing of Personal Data ("Official Gazette of the Re public of Macedonia" no. 7/05) 2005 Law on Personal Data Protec tion ("Official Gazette of the Republic of Macedonia" no. 7/05) For the purpose of further alignment with EU regulations, in February 2020 the Republic of North Macedonia adopted a new Law...

Match #58 76% similar

Automatic Processing of Personal Data, as well as the Law on Ratification of the Additional Protocol to the Convention for the Protection of Individuals with regard to automatic processing of

https://dijalogkoneu.mk/en/wp-content/uploads/sites/3/2021/10...

...process personal data of individuals who are EU citizens. [1] Available at: https://www. dzlp. mk/sites/default/files/pdf/Zakon_za_zastita_na_licnite_podatoci_2005. pdf [2] Available at: https://eur-lex. europa. eu/legal-content/EN/TXT/? uri=celex:31995L0046 [3] Available at: https://www. coe. int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37 [4] Available at: https://eur-lex. europa. eu/legal-content/EN/TXT/PDF/? uri=CELEX:02016R0679-20160504&from=EN [5] Available at: https://dzlp. mk/sites/default/files/u4/zakon_za_zastita_na_licnite_podatoci. pdf [6] Available at: https://dzlp. mk/sites/default/files/dzlp_strategija_mk. pdf Privacy ion **as** integral par t **of** developing qual i ty e ser vices an d tools 2 2008 **Law on Ratification of the Additional Protocol to the Convention for the Protection of Individuals with Regard to** Automated **Processing of Personal** Data Regarding Supervisory Authorities and Transborder Data Flows ("Official Gazette of the Republic of Macedonia" no. 103/08) 2016 General Data Protection Regulation 2016/679 2020 Law on Personal Data Protection ("Official Gazette of RNM" no. 42/20) 2005 Law on Ratification of the Convention for the Protection of Individuals with Regard to...

Match #59 64% similar

With the adoption of the new Personal Data Protection Law, there will be greater alignment with European regulations in the field of personal data protection, particularly the General Data Protection Regulation 2016/679

https://dijalogkoneu.mk/en/wp-content/uploads/sites/3/2021/10...

...Protection of Individuals with Regard to Automatic Processing of Personal Data ("Official Gazette of the Republic of Macedonia" no. 7/05) 2005 Law on Personal Data Protection ("Official Gazette of the Republic of Macedonia" no. 7/05) For the purpose of further alignment with EU regulations, in February 2020 the Republic **of** North Macedonia adopted a **new Law** on **Personal Data Protection** ("Official Gazette **of** RNM" no. 42/20)[5] that implied a transitional period for full application **in** duration **of** 18 months, i. e. **the law** enters into effect on August 24th, 2021. **The new Law** on **Personal Data Protection** is fully aligned **with the General Data Protection Regulation 2016/679,** for partial attainment of the strategic goal no. 1 ("Republic of Macedonia...

Match #60 62% similar

The Law on Personal Data Protection regulates the right to personal data protection as a fundamental freedom and right of natural persons and clearly defines the scope of personal data protection, i

https://dijalogkoneu.mk/en/wp-content/uploads/sites/3/2021/10...

...with citizens, thus making it necessary to find the right models for systems of personal data protection and security. Common denominator for all eservices that should be taken into account by all institutions is the need to secure continuous supervision of technical and organizational measures they implement in respect **to protection of personal data** relating **to** citizens that are subject **of** their processing operations. Introduction This policy document provides an overview **of the** standards **on personal data protection, as** stipulated under **the Law on Personal Data Protection** of RNM" no. 42/20) and the General Data Protection Regulation (GDPR), in respect to planning, creating and introducing eservices by institutions, and challenges standing on the path of the institutions in introducing such standards. 1 PRIVACY PROTECTION AS INTEGRAL PART OF DEVELOPING QUALITY E-SERVICES AND TOOLS 1. Alignment of the...

Match #61 87% similar

The law applies to all cases of fully or partially automated personal data processing

https://transparency.mk/wp-content/uploads/2022/02/fight_mo...

...in order to harmonize their work with the new regulations. The Law harmonises with the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and sets out, among other things, principles related to data processing, lawful bases, and data subject rights., even though North Macedonia is not an EU Member State. **The Law applies to** wholly **or partially automated personal data processing,** controller or processor establishment in the territory of the Republic of North Macedonia, as well as whether the data is processed on the territory of the Republic of North Macedonia or beyond its borders. Also, the Law is almost entirely aligned with the GDPR, but derogations are mainly introduced in...

Match #62 60% similar

of personal data, genetic data, biometric data, and data related to human health; - Technical and integrated processing of personal data (data protection by design and by default); - Personal

https://www.anonos.com/identifying-data-maybe-unlawful-gdpr...

...servers on which processing occurs, due to the potential acces s to such data by third country government agencies. [4] Use Ca se 2: Transfer of Pseudonymised Data at Paragraphs 85- 89 of th e EDPB Final Guidance. See also Italian university dissertation on this subject at https://www. SchremsII. com/epilogue. [5] mandat ory obligations **to** implement **technical and** organizational contr ols that enforce the principles relating **to processing of person al data, data protection by design and** default, **and** security **of processing** to all processing- both internal and external to th e EU. See GDPR Articles 5, 25 and 32 and Note 1, at Paragraphs 76 and 83. [6] See https://www. zdnet. com/article/amazon-fined-887-million-for-gdpr-privacy-violations/ [7] See https://www. wsj. com/articles/amazon-hit-with-record-eu-privacy-fine-1162764614 4 [8] As made clear in the case filed by Privacy International agai nst Acxiom and...

Match #63 65% similar

data protection impact assessment (DPIA) and - The certification and code of conduct are introduced

https://eridirect.com/files/GDPR-FAQ-Document-05312018.pdf

...the destruction of hardware with personal data stored on the d rives, it should highly consider establishing a Data Protection Offi cer role to establish systematic reviews and governance oversigh t. This person will be required to have "expert knowledge of data protection law and practices.".• ERI should conduct a full **Data P rotection Impact Assessment** (DPIA). An article by Medium Co rporation about GDPR Controllers **and** the following factors when conducting a DPIA 13 1. A systematic process of processing. 2. T he purpose of the processing. 3. Assess the purpose and the proc ess of processing. 4. Assess the risk related to individual's right t o freedom. 5. Measures to mitigate possible risk.• Overall, enforc ement action is...

Match #64 67% similar

The new Personal Data Protection Law promotes the principle of accountability, which requires controllers to be able to demonstrate compliance with the law

https://globaldatareview.com/guide/the-guide-data-critical-asse...

...the most comprehensive data protection laws in the world and is deemed by many to be the gold standard for laws regulating t he processing of personal data. It is no surprise, therefore, that t he drafting of data protection laws in many countries has been in spired by the GDPR.[3]One similarity GDPR and **the data protec tion** laws in many countries is **the** idea **of accountability, whic h** reflects **the** obligation **of the data** controller **to be** responsibl e for, and **to be able to demonstrate, compliance with the l aw.** words, simply complying with the law is not enough: data co ntrollers must be able to effectively show that they are complyin g with the law. To do that, creating documentation is fundamenta l. In some situations, it may also be one of the main obligations o f data controllers, such as having records...

Match #65 66% similar

In terms of the application of technical and organizational measures, a novel feature is that they are now designed and implemented in accordance with several criteria that take into account the nature, scope, context, and objectives of the processing, as well as the risks of varying probability and seriousness to natural persons' rights and freedoms

http://arno.uvt.nl/show.cgi?fid=155418

...risk should be understood broadly as referring to all the rights and freedoms of data subjects as intended in the European legisl ator's wording. 116 Recital 4 explains that, in the context of the GDPR, rights and freedoms are referred to: "all fundamental 114 Katerina Demetzou, 'Risks to the Rights **and Freedoms' A** Legal Interpretation **of the Scope of** Risk under **the** GDPR', **in** Data Pr otection **and** Privacy, Data Protection **and** Democracy 115 ibid 1 16 European Parliament **and of the** Council (n 9), Article 24(1) :" Taking **into account the nature, scope, context and** purpose s **of processing as well as the risks of varying** likelihood **an d** severity for **the rights and freedoms of natural** persons..." 34 **rights and** observes **the freedoms and** principles recognize d **in** the Charter as enshrined in the Treaties." The concept of risk is used in the GDPR as a criterion for forming legal obligations. T his has led legal scholars to speak about the EU data protection l egislation in terms of "riscification."117 Moreover, risk has emerg ed as a key criterion in the...

Match #66 61% similar

According to the "state of the art technology" approach, technical and integrated processing of personal data (Data protection by design and by default) is designed based on controller responsibilities:,

https://www.anonos.com/identifying-data-maybe-unlawful-gdpr...

...location of the servers on which processing occurs, due to the potential access to such data by third country government agencies. [4] Use Case 2: Transfer of Pseudonymised Data at Paragraphs 85- 89 of the EDPB Final Guidance. See also Italian university dissertation on this subject at https://www. SchremsII. [5] **The** GDPR mandatory obligations **to** implement **technical and** organizational controls that enforce **the** principles relating **to processing of personal data, data protection by design and default, and** security **of processing** apply **to** all **processing** both internal **and** to the EU. See GDPR Articles 5, 25 and 32 and Note 1, at Paragraphs 76 and 83. [6] See https://www. zdnet. com/article/amazon-fined-887-million-for-gdpr-privacy-violations/ [7] See https://www. wsj. com/articles/amazon-hit-with-record-eu-privacy-fine-11627646144 [8] As made clear in the case filed by Privacy International against Acxiom and Oracle (data brokers), Equifax and Experian (credit reference...

Match #67 71% similar

which can be classified into two parts: first, at the time of defining the means of processing, as well as at the time of processing, to apply appropriate technical and

https://irisbh.com.br/en/personal-data-and-anglicism-in-brazil-a...

...default": Article 25. Data protection by design and by default Taking into account the most advanced techniques, the costs of their application, and the nature, scope, context and purposes of data processing, as well as the risks arising from the processing to the rights and freedoms of individuals, whose **the** controller applies, both **at the time of defining the means of processing and at the time of the processing** itself, **the appropriate technical and** measures, such as pseudonymisation, aimed at effectively applying the principles of data protection. data, such as minimization, and to include the necessary guarantees in the treatment, in a way that it complies with the requirements of this regulation and protects the rights of data subjects. The controller applies technical and...

Match #68 60% similar

Regarding the Data Protection Impact Assessment, which is also a significant novelty, the Law requires an impact assessment whenever new technologies are used for some type of personal data processing and, at the same time, taking into account the nature, scope, context, and objectives of the treatment, it is likely to pose a high risk to individuals' rights and freedoms

https://transparency.mk/wp-content/uploads/2022/02/fight_mo...

...Another data processing activity where the Agency's approval is required, is personal data transfers outside of North Macedonia to non-EU/EEA countries. The approval by the Agency should be obtained in addition to the application of one of the respective legal grounds for transfers as per the GDPR. Requirements to Agency Transfers **of personal data to** countries within **the** EU/EEA **are** subject **to** prior notification **of the** Agency. **The scope and** form **of** such notification **are** still unclear. **Data** controllers **are** further obliged **to** notify **the** Agency if **the processing of personal data is likely to pose a high risk to the rights and freedoms of individuals (taking into account the nature, scope, context and** purposes **of the** processing). **The** Agency would maintain **a** record **of** all such **risk processing** activities in **the** country. Special Requirements **for Data Protection** ("DPO") Only individuals who meet the locally set criteria can act as DPOs, in particular: the DPO shall be fluent in the North Macedonian language, shall have a completed higher educational degree and may not be impeded by a sentence, court order or administrative sanction from practicing a specific profession....

Match #69 66% similar

As a result, the Law requires that the assessment be carried out in the case of a systematic and comprehensive assessment of personal aspects relating to natural persons that is based on automatic processing, including profiling

https://practiceguides.chambers.com/practice-guides/data-prot...

...regular and systematic monitoring of data subjects on a large scale; orthe core activities of the controller or the processor consist of the large-scale processing of special categories of data and personal data relating to criminal convictions and offences (Article 56 of the PDPA). Data Protection Impact AssessmentsThe data also obliged **to** perform **a** data protection impact **assessment in** cases where any **of the** following occur: **a systematic and** extensive evaluation **of personal aspects relating to natural persons that is based on** automated **processing, including profiling, and on** decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; large-scale processing of special categories of data or of personal data relating to criminal convictions and offences; or systematic monitoring of a publicly accessible area on a large scale (Articles 54 and...

Match #70 62% similar

The Law strengthens the position of the Data Protection Officer and introduces an obligation for the controllers to always appoint a personal data protection officer when:the processing is performed

http://web.archive.org/web/20220117135244/http://fox-electro...

...contact the Personal Data Protection Officer in connection with all issues related to the processing of their personal data, as well as in connection with the exercise of their rights prescribed by th is Law. 12. 1 The relationship between the Company as the contr oller and a Personal Data Protection **Officer The** bodies **of the** C ompany **appoint a Personal Data Protection Officer** from am ong their employees. **The** Company, as **the** controller, has **the o bligation to** timely **and** appropriately include **the Personal Da ta Protection Officer** in all matters related **to the protection of personal data.** this obligation, the Company needs to enable this person to perform all obligations by providing him/her with t he necessary means to perform these obligations, access to pers onal data and processing operations, as well as his/her professio nal development. The company must provide the Personal Data Protection Officer with independence in the...

Match #71 74% similar

by the state authorities;the basic activities of the controller or processor consist of processing operations, which due to their nature, scope and / or objectives, require to a large extent

https://transparency.mk/wp-content/uploads/2022/02/fight_mo...

...not have an 53 obligation to appoint a Data Protection Officer (DPO) if (i) it does not have more than 10 employees, or (ii) the pr ocessing refers to the personal data of members of associations f ounded for political, philosophical, religious or trade-union purpo ses. The Law provides that the DPO have **to** be appointed when **t he** core **activities of the controller or processor consist of processing operations which, by their nature, scope or** pur pose, **require** regular **and** systematic monitoring **of** data subjec ts or processing of special categories of data or processing of per sonal data related to criminal convictions and criminal acts speci fied in the Law. Conclusion Article 16 of the Treaty on the Functio ning of the European Union (TFEU) conferred very broad compet ences to the Union to legislate on data...

Match #72 81% similar

regular and systematic monitoring of personal data subjects; orthe basic activities of the controller or processor consist of extensive processing of special categories of personal data or personal data related

https://practiceguides.chambers.com/practice-guides/data-prot...

...are obliged to designate if:the processing is carried out by a pu blic authority or body, except for courts acting in their judicial ca pacity;the core activities of the controller or the processor consis t of processing operations that- by virtue of their nature, their sc ope and/or their purposes- require **regular and systematic mo nitoring of data subjects** on a large scale; **orthe** core **activiti es of the controller or the processor consist of the** large sc ale **processing of special categories of data and personal d ata** and offences (Article 56 of the PDPA). Data Protection Impact AssessmentsThe data controller is also obliged to perform a data protection impact assessment in cases where any of the followin g occur: a systematic and extensive evaluation of personal aspec ts relating to natural persons that is based on automated process ing, including...

Match #73 60% similar

e., harmonize their work with the new Law on Personal Data Protection

https://transparency.mk/wp-content/uploads/2022/02/fight_mo...

...a new level of security in the use and processing of users' pers onal data. GDPR has raised awareness in relation to the concept of privacy, and the draconic sanctions have pressured the compa nies to strive to achieve a new level of security in using and proc essing personal data. In 2020, **the** Republic of North Macedonia adopted **the new Law on Personal Data Protection,** in order to harmonize the existing legal framework in the field of protecti on of personal data with the GDPR standards. The law prescribes a time period of 18 months in which the controllers and processo rs are obliged to comply their work with the provisions of the ne w law, that...

Match #74 60% similar

the personal data processing, as well as the risks, with varying probability and seriousness, to the rights and freedoms of natural persons (personal data subjects) arising from that processing, and

http://arno.uvt.nl/show.cgi?fid=155418

...fundamental 114 Katerina Demetzou, 'Risks to the Rights and F reedoms' A Legal Interpretation of the Scope of Risk under the G DPR', in Data Protection and Privacy, Data Protection and Democ racy 115 ibid 116 European Parliament and of the Council (n 9), Article 24(1) :"Taking into account the nature, scope, purposes **of processing as well as the risks of varying** likelihood **and** sev erity for **the rights and freedoms of natural** persons..." 34 **rig hts and** observes **the freedoms and** principles recognized in **t he** Charter **as** in the Treaties." The concept of risk is used in the GDPR as a criterion for forming legal obligations. This has led leg al scholars to speak about the EU data protection legislation in te rms of "riscification."117 Moreover, risk has emerged as a key cri terion in the modified GDPR compliance scheme...

Match #75 78% similar

e., deletion of the different categories of personal data

http://web.archive.org/web/20210420142236/https://saulesmie...

...DATA SUBJECTS 6. 1. Before processing the Personal Data, the Data Controller shall provide the Data Subjects with the following information, in writing or by other means, including, where appro priate, in electronic form: (a) the name, details and contact detail s of the controller; (b) the purposes of the processing; (c) on **the** relevant **categories of Personal Data;** (d) the legal basis for th e processing of personal data; (e) the period for which the perso nal data will be stored or, if that is not possible, the criteria for d etermining that period; (f) The right to request that the Data Con troller grant access to the Personal Data of...

Match #76 66% similar

advise the controller or processor and the employees who perform processing in accordance with their obligations; to monitor compliance with the Law on Personal Data Protection, other relevant laws related

https://www.linkedin.com/pulse/gdpr-data-protection-officer-ko...

...privacy officers are like compliance officers (they can even be both in the compliance department). Less good combinations are e. g. head of Legal and DPOr, or CISO/BISO and DPOr. The tasks o f the data protection officer (art. 39 GDPR): These are the minim um tasks:- To inform and **advise the controller (or processor) and the employees who** carry out **processing** of **their obliga tions to** Privacy **law; To monitor compliance with the** GDPR **(or other** privacy laws), including **the** assignment of responsibilit ies, awareness raising **and** training of staff, and the related audit s;- To provide advice where requested as regards the Privacy Imp act Assessments and monitor its performance;- To cooperate wit h supervisory authorities- To act as contact point for the supervis ory authorities on processing issues (especially those where prior consultation of the supervisory...

Match #77 67% similar

nature, scope, context and objectives of processing, as well as risks with different degree of probability and seriousness of the rights and freedoms of individuals, are obliged to apply appropriate

http://web.archive.org/web/20201201053727/https://www.dfele...

...the regulations on data protection. Security The security meas ures adopted by DF Electric, S. A. are those required, in accordan ce with the provisions of article 32 of the RGPD. In this regard, D F Electric, S. A., taking into account the state of technology, the costs of application, and the **nature, scope, context, and** purp oses **of the** data **processing, as well as the risks of** variable **probability and seriousness of the rights and freedoms of** natural persons, has established **the appropriate** technical **and** measures to ensure the level of security appropriate to the existi ng risk. In any case, DF Electric, S. A. has enough mechanisms in place to: Guarantee the permanent confidentiality, integrity, avai lability, and resilience of data processing systems and services. Quickly restore availability and access to personal data, in case o f...

Match #78 100% similar

technical and organizational measures to ensure a level of security appropriate to the risk

https://medium.com/golden-data/territorial-scope-of-eu-data-pr...

...applicable, the processor shall maintain a record of all categori es of processing carried out on behalf of a controller, as per Articl e 30(2). Where applicable, the processor shall, upon request, coo perate with the supervisory authority in the performance of its ta sks, as per Article 31. The processor shall implement **technical and organizational measures to ensure a level of security appropriate to the risk,** as per Article 32. The processor shall notify the controller without undue delay after becoming aware o f a personal data breach, as per Article 33. Where applicable, the processor shall designate a data protection officer as per Articles 37 and 38. The provisions on transfers of personal data to...

Match #79 63% similar

On the other side, entities planning or dealing with e-commerce are required to apply appropriate technical and organizational measures to ensure a level of security in accordance with the

https://globaldatahub.taylorwessing.com/article/gdpr-cybersec...

...HomeHot topicsArticlesNewsToolsVideosEventsServicesContact GDPR cybersecurity and breach reporting requirementsDebbie H eywood sets out the main provisions around cybersecurity and b reach reporting under the GDPR and looks at regulator guidance. GDPR covers **security and** breach reporting **in** relation **to** perso nal data **in** Articles 32-34. SecurityControllers **and** processors **ar e required to** implement **appropriate technical and** organisat ional **measures to ensure a level of security appropriate to the** risk. **The** assessment of what might be appropriate involves considering the context and purposes of the processing as well a s the risk of varying likelihood and severity for the rights and free doms of individuals. Appropriate measures are set out as possibl y including:pseudonymisation and encryption;ensuring confidenti ality, integrity, availability and resilience of processing systems...

Match #80 67% similar

Law on Personal Data Protection and taking into account the latest technological advances, implementation costs, and the nature, scope, context, and objectives of processing, as well as risks with varying

https://caberseg.com/en/the-supreme-court-rules-on-security-...

...a way as to ensure appropriate security of personal data, inclu ding protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, by implementing appropriate technical or organizational measures". But how to en sure that security? Well, the GDPR itself provides an answer: "Co ntrollers and processors shall determine **and** adopt measures ap propriate to **the** existing risk, **"Taking into account the** state **o f the** art, **the costs of implementation, and the nature, sco pe, context and** purposes **of the processing, as well as risk s of varying** likelihood **and** to the rights and freedoms of natura l persons." The problem with these provisions is obvious; at no ti me is the specific content of these measures specified. Instead, i t is up to the data subjects themselves to carry out the relevant r isk analysis and, consequently, to implement the necessary mea sures to...

Match #81 70% similar

degrees of probability and seriousness to individuals' rights and freedoms

http://web.archive.org/web/20210420142236/https://saulesmie...

...any other unlawful processing, both when establishing the Dat a Processing Measures and during the Data Processing itself. 14. 2. The controller must act taking into account the level of develo pment of technical possibilities, implementation costs and the na ture, scope, context and purposes of the processing of personal data, as various probabilities **and seriousness of** the processin g **of** personal data **to individuals' rights and freedoms.** 14. 3. Customized Personal Data Protection means that any new applic ation or system that uses Personal Data must be designed with t he protection of such Personal Data in mind. Privacy must be tak en into account throughout the life of the program or system. 14. 4. The measures that should...

Match #82 62% similar

According to the Albanian Constitution, the protection of personal data in Albania is currently governed by Law "On the Protection of Personal Data no

http://web.archive.org/web/20220331110234/https://www.hakl...

...About the programme Logos and Guides Application Guidelines Application Documents Visibility Guide Rights Based Approach Tr ansparency Policy Data and Privacy Policy Branding and logos Gr antee CSOs Capacity Building& Support About Support Program me Mentoring and Expert Support Notice and consent text regar ding **the** processing **of personal data** What **is** LPPD? LPPD **is th e Law on the Protection of Personal Data no.** 6698 issued **in** order to protect the fundamental rights and freedoms of people, particularly the right to privacy, with respect to the processing of personal data, and to set forth obligations of natural and legal pe rsons who process personal data. Within the scope of the law, pe rsonal data is defined as "all the...

Match #83 61% similar

We consider that the special law, which incorporates and develop the main principles and standards of personal data control, as well as the role of the Data Protection Commissioner as the primary authority, thereby establishing a comprehensive regulatory and institutional framework for data privacy

https://openknowledge.worldbank.org/bitstream/handle/10986/...

...practices, and policies with respect to personal data• Individua l participation principle: the data subject should have the right to request data from a data controller or a confirmation of whether the data controller has personal data relating to the individual. If the data controller has such data, it provided to **the data** subjec t within **a** reasonable time, in **a** reasonable manner **and** in **a** for m **that** is readily intelligible to **the data** subject Accountability p rinciple: **the data** controller should be held accountable **for** abid ing with **principles of the** Guidelines 107 Albania has implemen ted an advanced **and comprehensive regulatory and institut ional framework for data privacy.** the EU, Albania adopted a new Law on Protection of Personal Data in 2008, which mandate d the establishment of the Information and Data Protection Com missioner (IDPC) as the main authority charged with policy maki ng and regulating personal data in Albania. The Law on Protectio n of Personal Data incorporates the main...

Match #84 66% similar

Moreover, a thorough examination of the law reveals that Albania follows the EU model by allowing personal data transfers to jurisdictions that provide an adequate level of protection on the basis of contractual obligations, allowing businesses to outsource some of their data management needs

https://openknowledge.worldbank.org/bitstream/handle/10986/...

...covers all main regulatory areas of digital privacy. First, specific rules govern sensitive personal data, such as political views, sex ual orientation, medical history, religion, or ethnical origin- there by safeguarding deeply personal values and preventing discrimin ation or other forms of misuse. Second, the law specifies that leg itimate reason is and processing **personal data. The** central req uirement is obtaining **the** consent **of the data** subject. In additi on **to** consent, **some** additional **basis** for **the** collection and proc essing **of data** is possible under **the law. Allowing** for **data to** be transferred and processed **on the basis of contractual obli gations** allows **businesses to outsource some of their data management needs,** or consumer analytics. A strong public pu rpose can override the need to seek consent. 65 Third, the law e nshrines the ability to retrieve one's personal information, reques t its amendment or demand its deletion as an essential right of d ata subjects. Fourth, the law includes guidance on the conditions for...

Match #85 100% similar

ability to retrieve one's personal information, request its amendment, or demand its deletion

https://openknowledge.worldbank.org/bitstream/handle/10986/...

...law. Allowing for data to be transferred and processed on the b asis of contractual obligations allows businesses to outsource so me of their data management needs, such as HR, payroll, or con sumer analytics. A strong public purpose can override the need t o seek consent. 65 Third, the law enshrines the **ability to retrie ve one's personal information, request its amendment or demand its deletion** as an essential right of data subjects. Four th, the law includes guidance on the conditions for data to be tra nsferred to other jurisdictions. In this context, Albania follows the EU model of allowing transfers of personal data to jurisdictions th at offer an "adequate level of protection". Transfer of personal da ta...

Match #86 60% similar

scope of the law on the controllers established in the Republic of Albania, the diplomatic missions or consular offices of the Albanian state and controllers who are not established in

https://www.etd.ceu.edu/2021/zotaj_sara.pdf

...also the enforcement one, Albanian legislation provides for the necessary protection of personal data. The necessary protection is supplemented by the secondary legislation adopted by the Co uncil of Ministers and the Commissioner as well. The Law provide s that it will be applicable to the processing of data by controllers 25 **established in the Republic of Albania and controllers who are not established in the Republic of Albania** but that use equipment situated **in the Republic of Albania.** 26 **The La w** has tried to cover **not** only **the** processing **of** data by **Albania n controllers,** but also by foreign **controllers** using equipment **in Albania,** but the Law does not clarify whether it applies to the processing of the data of Albanian citizens by controllers not esta blished in Albania. Meanwhile the GDPR makes it clear its extrate rritorial scope by applying even to companies that are not establi shed in the EU, but "that use personal...

Match #87 100% similar

the Republic of Albania, making use of any equipment situated in the Republic of Albania

http://web.archive.org/web/20220117221346/https://cms.law/e...

...means of a personal data stored in a filing system, or intended to form part of a filing system. This law shall apply to the process ing of personal data by:controllers established in the Republic of Albania;diplomatic missions or consular offices of the Albanian st ate;controllers who are not established in **the Republic of Alba nia, making use of any equipment situated in the Republic of Albania;** In circumstances stipulated in point 3, the controller designates a representative established in the territory of Albani a. Stipulations of this law applying to controllers are also applica ble to their representatives. This law applies also to the public au thorities that process personal data. This law is not applicable to processing...

Match #88 82% similar

Beside this, in a comparative overview of the GDPR which extend it appliance in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not

http://web.archive.org/web/20210421205831/https://practicalp...

...whether there was a sufficient legal basis to serve the claims o utside the UK. A key element of that inquiry was whether Forensi c News's personal data processing underlying Soriano's data prot ection claims was subject to GDPR under Article 3. Article 3. 1, **G DPR** "applies to **the processing of** personal data **in the conte xt of the activities of an establishment of a controller or a processor in the Union, regardless of whether the process ing takes place in the Union or** 22 describes an establishment as implying "the effective and real exercise of activity through st able arrangements." Soriano argued that several factors showed Forensic News conducted such processing and had stable arrang ements in the UK. These factors included Forensic News publishi ng its stories in English (the language used in the UK),...

Match #89 92% similar

As a result, the regulation applies to the processing of personal data of data subjects in the Union by a controller or processor not established in the Union, where

http://web.archive.org/web/20210928000146/https://www.priva...

...of personal data in the context of the activities of an establish ment of a controller or a processor in the Union, regardless of wh ether the processing takes place in the Union or not. Dossier: Est ablishment NEW: The practical guide PrivazyPlan explains all dat aprotection obligations and helps you to be compliant. 2. This **Re gulation applies to the processing of personal data of dat a subjects** who are **in the Union by a controller or processo r not established in the Union, where** the processing activitie s are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such dat a subjects in the Union; or (b) the monitoring of their behaviour a s far as their behaviour takes place within the Union. 3. This...

Match #90 90% similar

the processing activities are related to the offering of goods or services to such data subjects in the Union, regardless of whether payment of the data subject is required, or

http://web.archive.org/web/20210421205831/https://practicalp...

...Goods or Services Criterion GDPR Article 3. 2 extends GDPR's t erritorial reach to organizations without an EU establishment und er two circumstances. First, Article 3. 2(a) provides that GDPR ap plies to personal data processing of individuals located in the Eur opean Union by controllers or processors without an EU establish ment "where **the processing activities are related to the off ering of goods or services,** irrespective **of whether** a **payme nt of the data subject is required, to such data subjects in the Union.**" Soriano argued that Forensic News's offering of serv ices to UK readers met that standard, relying on the same facts c ited for his Article 3. 1 establishment argument. But that argume nt also failed to persuade the court. The court explained that "no more than cursory examination" of the facts showed...

Match #91 76% similar

monitoring of their behavior as far as their activity occur within the Union

http://web.archive.org/web/20210928000146/https://www.priva...

...are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union ; or (b) the **monitoring of their** behaviour **as far as their** beha viour takes place **within the Union.** 3. This Regulation applies t o the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by v irtue of public international law. This page can also be addressed https://www. privacy-regulation. eu/en/3. htm. BG- CS- DA -...

Match #92 90% similar

Taking into consideration extraterritorial application of the GDPR, Albanian Law would have to reconsider the territorial scope of application to controllers not established in Albania, but that process data of Albanian citizens

https://www.etd.ceu.edu/2021/zotaj_sara.pdf

...abroad. 28 Even though the extraterritorial application of the G DPR might raise issues29 because of the broad interpretation giv en to the clause, the GDPR has tried to clarify30 that there are v arious factors to be considered in deciding whether the GDPR will apply to controllers not established in the Union. **Taking into co nsideration** these clarifications **of the GDPR, Albanian Law w ould have to reconsider the territorial scope of applicatio n to controllers not established in Albania, but that proce ss data of Albanian citizens.** This **application** of the law for t he processing of data of Albanian citizens should be seen in the li ght of the new technological developments, which make it easier for the processing of the data to happen everywhere, regardless of the physical presence in a specific territory. In order to adapt t o these...

Match #93 100% similar

This application of the law for the processing of data of Albanian citizens should be seen in the light of the new technological developments, which make it easier for the processing of the data to happen everywhere, regardless of the physical presence in a specific territory

https://www.etd.ceu.edu/2021/zotaj_sara.pdf

...factors to be considered in deciding whether the GDPR will app ly to controllers not established in the Union. Taking into consider ation these clarifications of the GDPR, Albanian Law would have t o reconsider the territorial scope of application to controllers not established in Albania, but that process data of Albanian citizens. **This application of the law for the processing of data of Al banian citizens should be seen in the light of the new tech nological developments, which make it easier for the proc essing of the data to happen everywhere, regardless of th e physical presence in a specific territory.** In order to adapt to these rapidly changing technologies that enable the processin g to take place everywhere, Albania would have to amend the la w. The amendment is needed in order to equally protect all Alban ian citizens, without making a difference on their rights just beca use the controller is not...

Match #94 100% similar

In order to adapt to these rapidly changing technologies that enable the processing to take place everywhere, Albania would have to amend the law

https://www.etd.ceu.edu/2021/zotaj_sara.pdf

...data of Albanian citizens. This application of the law for the pro cessing of data of Albanian citizens should be seen in the light of the new technological developments, which make it easier for th e processing of the data to happen everywhere, regardless of the physical presence in a specific territory. **In order to adapt to th ese rapidly changing technologies that enable the proces sing to take place everywhere, Albania would have to ame nd the law.** The amendment is needed in order to equally prote ct all Albanian citizens, without making a difference on their right s just because the controller is not established in Albania, but wh ich nevertheless constitutes a breach of personal data. 28 Article 3(2) of the GDPR. 29 Toby Blyth and Jessica Yazbek,...

Match #95 100% similar

The amendment is needed in order to equally protect all Albanian citizens, without making a difference on their rights just because the controller is not established in Albania, but which nevertheless constitutes a breach of personal data

https://www.etd.ceu.edu/2021/zotaj_sara.pdf

...the new technological developments, which make it easier for t he processing of the data to happen everywhere, regardless of th e physical presence in a specific territory. In order to adapt to the se rapidly changing technologies that enable the processing to t ake place everywhere, Albania would have to amend the law. **Th e amendment is needed in order to equally protect all Alb anian citizens, without making a difference on their rights just because the controller is not established in Albania, b ut which nevertheless constitutes a breach of personal da ta.** 28 Article 3(2) of the GDPR. 29 Toby Blyth and Jessica Yazbek, Does the EU's General Data Protection Regulation have extra-terr itorial effect?, 16 November 2020. 30 Recital 23 of the General D ata Protection Regulation. C E U eT D C ol le ct io n 5 CHAPTER II SPECIFIC...

Match #96 70% similar

As it was mentioned the consent of the data subject represents the declaration of the data subject’s will by a statement or by a clear affirmative action, which signifies agreement to the processing of personal data relating to him or her

http://web.archive.org/web/20210513222835/https://designit.ie...

...the DPC will start issuing fines to companies that do not compl y. Have you checked your website recently? Does it comply with t he current ePrivacy and GDPR regulations? So what has actually changed since GDPR was introduced in 2018? The original law on cookies has not changed. What has is **the** definition **of consent to** process **personal data. The** new definition **of consent** is: **"i t** must be freely given, specific, informed and unambiguous, **by a statement or by a clear affirmative action, which signifi es agreement to the processing of personal data relating to him or** her". **As a** of the revised regulation (ePrivacy directive), the user must: be able to consent to or reject having cookies s et be provided with clear and comprehensive information about each cookie before consenting/rejecting be provided with the opt ion to choose which cookies they are consenting to/rejecting be a ble to change/withdraw their consent...

Match #97 84% similar

If the controller or processor processes personal data for the purpose of offering business opportunities or services, the data must be taken from a public list of data

https://www.etd.ceu.edu/2021/zotaj_sara.pdf

...came from publicly accessible sources, and that the term publi c domain has no relevance in data protection regulation. 40 The Regulation therefore recognizes the protection of personal data, even those collected through public sources. On the other hand, Article 6(3) of the Albanian Law states that the processing is **if t he controller** carries out **personal data** processing **for the pu rpose of offering business opportunities or services,** provi ded that **the data** were **taken from a public list of data.** of th e GDPR. 38 See the decision of the Polish Data Protection Authori ty (DPA) of 25 March 2019. 39 Article 6 of the Law no. 9877. 40 A rticle 14(2)(f) of the General Data Protection Regulation. C E U eT D C ol le ct io n 7 While in the...

Match #98 90% similar

monitoring the adoption of "transparency programs" on the use of personal data by public authorities and supervising compliance by individual firms, either by investigating complaints received from individuals or conducting

https://openknowledge.worldbank.org/bitstream/handle/10986/...

...among ordinary Albanians and small businesses. Concerns abo ut how personal data is being used and protected have hindered the wide adoption of e-government services in Albania. 66 Most of IDPC's focus is geared toward promoting implementation of da ta protection rules by government and private entities. To that en d, it **the adoption of "transparency** programmes" **on the use of personal data by public authorities and** oversees **compli ance by individual firms either by investigating complaint s received from individuals or by conducting** own ex officio i nvestigations. IDPC's outreach to civil society supports these goa ls. Yet consultations with stakeholders and experts suggests that the level of awareness of Albania's data protection regimes by in dividuals and small businesses (including those in the IT sector) r emains low, curtailing individuals' trust in Albania's e-commerce and other...

Match #99 76% similar

their own ex officio investigations. However, consultations with stakeholders and experts indicate that individual and small business awareness of Albania's data protection regimes remains low, limiting individuals' trust in Albania's e-commerce and other digital firms

https://openknowledge.worldbank.org/bitstream/handle/10986/...

...is geared toward promoting implementation of data protection rules by government and private entities. To that end, it monitors the adoption of "transparency programmes" on the use of person al data by public authorities and oversees compliance by individ ual firms either by investigating complaints received from individ uals or by conducting **their own ex officio investigations.** IDP C's outreach to civil society supports these goals. Yet **consultati ons with stakeholders and experts** suggests **that** the level **o f awareness of Albania's data protection regimes** by **indivi duals and small** businesses (including those **in** the IT sector) **re mains low,** curtailing **individuals' trust in Albania's e comm erce and other digital firms.** Strengthen **data** protection awar eness-raising campaigns targeting ordinary Albanians and small businesses: IPDC may considering strengthening its awareness-r aising campaigns as a tool to both incentivize implementation by firms and to promote trust in Albania's emerging e-commerce se ctor. Public and private sector stakeholders could collaborate peri odically to share information on privacy and cybersecurity risks...

Match #100 70% similar

privacy laws and Federal Trade Commission settlements with companies, albeit in weaker, less prescriptive forms

https://docslib.org/doc/1365976/gdpr-eu-regulations-pdf

...consistent regulatory development in information policy in a ge neration. GDPR puts personal data into a complex and protective regulatory regime. However, the ideas contained in GDPR are not entirely European nor new. THE protection of GDPR can be found- albeit in weaker, less prescriptive forms- in U. S. **privacy laws a nd federal trade commission settlements with companies.** Although many **companies and** prepare and this, they changed their privacy policies and functions around the world just before t he introduction of GDPR, and usually provided emails and other n otifications discussing these changes. This has been criticized for leading to a quenching number of messages, while experts note d that some email reminders incorrectly argued...

Match #101 61% similar

They deal with e-commerce by implementing appropriate technical and organizational measures to ensure a level of security in accordance with the Law on Personal Data Protection, taking into account

https://www.salesforce.com/news/wp-content/uploads/sites/3/2...

...further. Portability of personal data: Data subjects also now hav e the right, in certain circumstances, to receive the personal dat a that they have provided to a Controller in a structured, commo nly used and machine-readable format. Salesforce's data process ing addendum takes into account these expanded and new right s. 3. Security measures: **The** GDPR requires Controllers **and** Proc essors **to** implement **appropriate technical and organization al measures to ensure a level of security appropriate to th e** risks presented. At Salesforce, we have robust **security meas ures in** place that meet **the** standards in the industry. For some of our services, we have security certifications including the Inter national Organization for Standardization (ISO) 27001 and 27018 standard, the American Institute of CPAs' (AICPA) System and Or ganization Controls (SOC) reports, the Payment Card Industry Da ta Security Standards (PCI), the TÜV Rheinland Certified Cloud Se rvice,...