AMERICAN UNIVERSITY OF ARMENIA
ՀԱՅԱՍՏԱՆԻ ԱՄԵՐԻԿՅԱՆ ՀԱՄԱԼՍԱՐԱՆ
LL.M. Program
ԻՐԱՎԱԳԻՏՈՒԹՅԱՆ ՄԱԳԻՍՏՐՈՍԻ ԾՐԱԳԻՐ

TITLE

Privacy Policy as a Tool for IT Companies to Escape Liability

STUDENT'S NAME

SHAHANE RUBEN EKSUZYAN

SUPERVISOR'S NAME

PROF. LILIT BANDURYAN

NUMBER OF WORDS

6998

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
law@aua.am

TABLE OF CONTENT

LIST OF ABBREVIATIONS **3**

INTRODUCTION **4**

CHAPTER 1 **7**

Major GDPR Violation by Data Controllers

CHAPTER 2 **17**

The Method to Avoid Liability

CONCLUSION **25**

BIBLIOGRAPHY **26**

40 Marshal Baghramyan Avenue

0019, Yerevan, Armenia

Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

law@aua.am

LIST OF ABBREVIATIONS

GDPR	General Data Protection Regulation
TFEU	Treaty on the Functioning of the European Union
BfDI	The General Commissioner of Data Protection and Freedom of Information
GmbH	Gesellschaft mit beschrankter Haftung (german for Limited Liability Company)
ICO	Information Commissioner
DPO	Data Protection Officer
HDPA	Hellenic Data Protection Authority

40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

INTRODUCTION

Privacy policy is a statement or a legal document (in privacy law) that states ways in which a company that acts as a data controller processes, i.e. gathers, uses, discloses, and in general, manages a customer's or client's data[1]. Usually, when being asked to provide our personal data to a controller we are required to get acquainted with such policies and give our consent. However, very few of us thoroughly read the "Legal terms and Conditions" agreement before agreeing to it. Privacy policy documents issued by data controllers are often overlooked by customers either because they are too long and boring, or because they contain too many technical details and are not legible. For example, Microsoft's privacy policy is 77 pages long.[2] In the article "The biggest Lie on the Internet: Ignoring Privacy Policies and Terms of Service Policies of Social Networking Services"[3] authors discuss a study aimed at getting an overall idea of how much Privacy Policies are read by the users. In this study authors created a fake social networking site called Name Drop with a terms and services agreement. The agreement included a disclosure that users give up their first-born child as payment. They found that 98% of participants agreed to this, meaning that 98% didn't actually read the privacy policy.

Since most users do not bother reading such agreements, there is a pressing need for some norms regulating privacy. Authors of the article "Analyzing GDPR Compliance through the Lens of Privacy Policy"[4] emphasize a demand for a standardized privacy-policy document for GDPR[5] (General Data Protection Regulation (Regulation (EU) 2016/679) -compliant

---

[1]Flavián, C., Guinalíu, M.: Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. Ind. Manag. Data Syst. 106(5), 601– 620 (2006)

[2]Microsoft privacy policy https://privacy.microsoft.com/en-us/privacystatement?PrintView=true (last accessed February 2020).

[3]Obar, Jonathan A. and Oeldorf-Hirsch, Anne, The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services (June 1, 2018). TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy, 2016.. Available at SSRN: https://ssrn.com/abstract=2757465 or http://dx.doi.org/10.2139/ssrn.2757465

[4]Mohan, J., Wasserman, M., & Chidambaram, V. (2019). Analyzing GDPR Compliance Through the Lens of Privacy Policy. *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*, 82-95. doi:10.1007/978-3-030-33752-0_6

[5]The GDPR is a law of European Union that entered into force in 2016. It became directly applicable in all Member States of the European Union on May 25, 2018. The regulation does not require implementation by the EU Member States through national law.

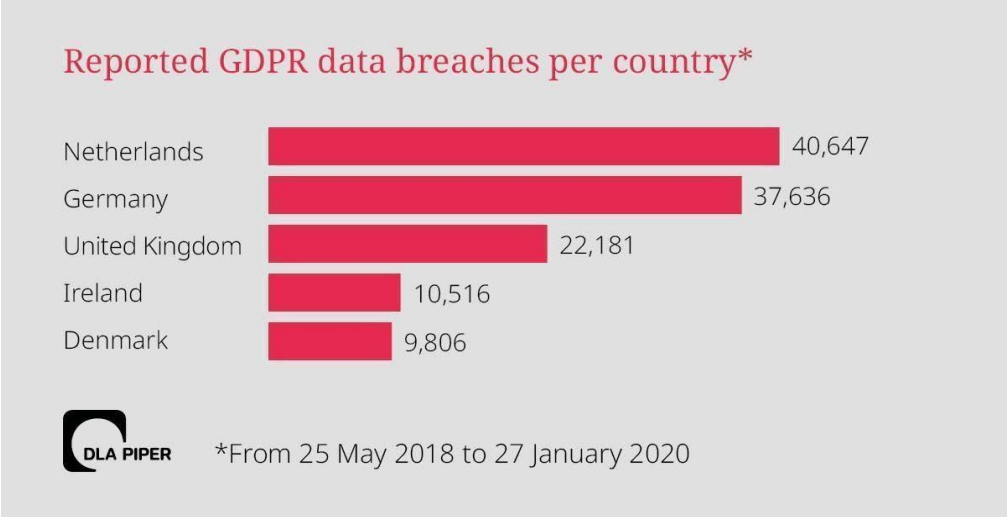
40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

systems. A GDPR compliant privacy policy would give confidence to data subjects because they will feel more secure and data controllers since they will be more protected. It will also exempt companies which process personal data, including IT companies from possible litigation.

Having such a legal shield can protect companies against huge financial losses. Failure to comply with GDPR could result in big fines. DLA Piper**,** which is a multinational law firm with offices in more than 40 countries throughout the Americas, Asia Pacific, Europe, Africa, and the Middle East[6], conducted a GDPR Data Breach Survey[7]. According to that survey, data protection regulators have imposed EUR114 million in fines under the GDPR regime for a wide range of GDPR infringements. The Netherlands, Germany and the UK topped the table of the number of data breaches notified to regulators (see picture 1).



Picture 1. Reported GDPR data breaches per country from 25 May 2018 to 27 January 2020[7].

The maximum fine according to the GDPR is as high as EUR20 million or, in case of undertaking, 4% of annual global turnover — whichever is greater.[8]

This paper is going to focus on GDPR-compliant privacy policy development for Armenia-based IT companies. The law on State Assistance of Information Technologies adopted in 2014 by the Republic of Armenia resulted in a sharp increase in Armenia-based IT

[6]DLA Piper. (2005, January 26). Retrieved from https://en.wikipedia.org/wiki/DLA_Piper#cite_note-facts-1
[7]GDPR fines. https://www.dlapiper.com/en/ireland/insights/publications/2020/01/gdpr-data-breach-survey-2020/ (last accessed February 2020)
[8]GDPR penalties and fines. https://www.itgovernance.co.uk/dpa-and-gdpr-penalties (last accessed March 2020)

40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

companies[9]. In 2017 the number of registered IT companies reached 272. Current ATOM (Advanced Tomorrow) Presidential Initiative on Technology and Science Development in Armenia, aims at leading IT companies from abroad to develop artificial intelligence, mathematical modeling and machine learning. [10]

With such a rapid growth of the number of IT companies in Armenia, tools are needed to ensure that they comply with GDPR standards while processing data of EU nationals and or transferring data to the EU territory. A GDPR-compliant privacy policy can be used as such a tool to escape possible litigations, which can result in big financial fines.

This thesis paper focuses on the development of GDPR-compliant Privacy Policy for IT companies to be used as a tool to escape liability. It consists of an introduction, two chapters, a conclusion and a bibliography. The Introduction is an overview of what is privacy policy, why it is needed, how IT companies can utilise it to escape liability which can, in some cases, exceed their annual turnover. **Chapter 1** uses the case study methodology to show the major drawbacks in privacy policies that lead to liability of companies. It analyzes most common fallacies in privacy policies that are found in breach of the GDPR. Stemming from Chapter 1, **Chapter 2** shows how the drawbacks identified in the first Chapter can be addressed based on the GDPR. As a result, we come up with an exemplary sample of a privacy policy that can be used by IT companies to decrease the number of cases initiated against them. Conclusion succinctly outlines the main findings of the research.

[9]"ՏԵՂԵԿԱՏՎԱԿԱՆ ՏԵԽՆՈԼՈԳԻԱՆԵՐԻ ՈԼՈՐՏԻ ՊԵՏԱԿԱՆ ԱՋԱԿՑՈՒԹՅԱՆ ՄԱՍԻՆ", available at https://www.arlis.am/DocumentView.aspx?docID=95017 (last accessed March 2020)

[10]Make Armenia a country of Modern technologies: President meets representatives of IT companies. https://en.armradio.am/2020/02/07/make-armenia-a-country-of-modern-technologies-president-meets-representatives-of-it-companies/ (last accessed February 2020)

40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia law@aua.am

CHAPTER 1

Major GDPR violation by data controllers

In this chapter I am going to use the case study methodology to show the major drawbacks in privacy policies that lead to liability of companies. First, let us see what type of fines exist and what is the statistics of fines.

There are two tiers of administrative fine for non-compliance with the GDPR:[11]

1. Up to €10 million, or, in the case of an undertaking, 2% of annual global turnover -whichever is greater - issued for infringement of the following GDPR articles:
   - Art. 8 (conditions for children's consent);
   - Art.11 (processing that doesn't require identification);
   - Arts.25 – 39 (general obligations of processors and controllers);
   - Art.42 (certification); and
   - Art.43 (certification bodies).
2. Up to €20 million, or, in the case of an undertaking, 4% of annual global turnover – whichever is greater, issued for infringement of the following GDPR articles:
   - Art.5 (data processing principles);
   - Art.6 (lawfulness of processing);
   - Art.7 (conditions for consent);
   - Art.9 (processing of special categories of data);
   - Arts.2 – 22 (data subjects rights); and
   - Art.44 – 49 (data transfers to third countries or international organizations).

The GDPR statistics of the most common breaches leading to violations of the GDPR are as follows[12]:

[11] GDPR penalties and fines. https://www.itgovernance.co.uk/dpa-and-gdpr-penalties (last accessed March 2020)
[12] Statistics of the fines by the types of violations https://www.enforcementtracker.com/?insights (last accessed March 2020)

40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia law@aua.am

1. Fines by total sum:

Violation	Number of Fines
Insufficient legal basis for data processing	**89** (with total sum of € 110,083,147)
Insufficient technical and organisational measures to ensure information security	**56** (with total sum of € 332,842,127)
Non-compliance with general data processing principles	**34** (with total sum of € 16,152,370)
Insufficient fulfilment of data subjects rights	**21** (with total sum of € 7,792,787)
Insufficient fulfilment of information obligations	**14** (with total sum of € 554,065)
Insufficient fulfilment of data breach notification obligations	**6** (with total sum of € 158,425)
Insufficient cooperation with supervisory authority	**6** (with total sum of € 18,511)
Insufficient data processing agreement	**2** (with total sum of € 14,380)
Lack of appointment of data protection officer	**2** (with total sum of € 61,000)
Unknown	**1** (with total sum of € 500)

2. By total number of fines:

Violation	Sum of Fines
Insufficient technical and organisational measures to ensure information security	**€ 332,842,127** (at 56 fines)
Insufficient legal basis for data processing	**€ 110,083,147** (at 89 fines)
Non-compliance with general data processing principles	**€ 16,152,370** (at 34 fines)
Insufficient fulfilment of data subjects rights	**€ 7,792,787** (at 21 fines)
Insufficient fulfilment of information obligations	**€ 554,065** (at 14 fines)
Insufficient fulfilment of data breach notification obligations	**€ 158,425** (at 6 fines)
Lack of appointment of data protection officer	**€ 61,000** (at 2 fines)
Insufficient cooperation with supervisory authority	**€ 18,511** (at 6 fines)
Insufficient data processing agreement	**€ 14,380** (at 2 fines)
Unknown	**€ 500** (at 1 fines)

As seen from the statistics, insufficient legal basis for data processing and insufficient technical and organizational measures to ensure information security and non-compliance with GDPR heads both tolls. Let us analyze each type of infringement of the GDPR.

Insufficient legal basis for data processing

Insufficient legal basis for data processing arises mainly in violation of articles 5 and 6 of the GDPR.

Article 5 of the GDPR concerns the principles relating to processing of personal data. According to it, personal data shall be processed (a) lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected

40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization'); (d) accurate and, where necessary, kept up to date ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

Article 6 defines the scope of lawfulness of data processing. The processing can be considered lawful only if (a) the data subject has given consent to the processing of his or her personal data; (b) processing is necessary for the performance of a contract to which the data subject is a part, (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The most common violations of those articles arise due to:

1. Publication of personal data. To showcase this let us discuss an Austrian case. The Austrian data protection imposed an administrative fine of EUR 18 million on Austrian Post after having carried out ordinary administrative criminal proceedings with a criminal penalty dated October 23, 2019.[13] Austrian Post created profiles of more than three million Austrians, which included information about their home addresses, personal preferences, habits and possible party affinity - which were subsequently resold. This violates both Articles 5 and 6, since Austrian Post collected obtained information for post services, however used it for another purpose, and shared information without consent of data subjects.

2. Non-compliance of personal data collection purpose with its usage:

[13]Datenschutzskandal: Millionenstrafe für Post https://wien.orf.at/stories/3019396/ (last accessed on March 2020).

40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

This is a violation of **articles 5(b)** and **6**. For instance, the Italian supervisory authority imposed two fines totaling EUR 11,5 million on Eni Gas e Luce 19 December 2019, for unlawful processing of personal data in the context of advertising activities and activation of unsolicited contracts.[14] In the course of 2018 and the first months of 2019, the Italian Authority received several dozen reports and complaints regarding receipt of promotional calls on behalf of Eni Gas e Luce, without obtaining prior consent of interested parties. It turned out that the Company carries out telemarketing activities and tele-selling through a network of agencies responsible for the processing of personal data. Telephone contacts were obtained from personal data of corporate customer database, or purchased from providers.

3. Selling personal data to third parties without consent of data subjects

An example of such violation is the case of The Dutch Data Protection Authority v Royal Dutch Tennis Association ("KNLTB")[15]. The latter was fined EUR 525,000 for selling personal data of more than 350,000 of its members to sponsors who had contacted some of the members by mail and telephone for direct marketing purposes. KNLTB sold the names, gender and addresses of their members to third parties without obtaining the consent of the data subjects. The data protection authority also rejected the existence of a legitimate interest for the sale of the data and therefore decided that there was no legal basis for the transfer of personal data to the sponsors. This case was found to violate Article 5(b), which describes the purpose limitation, and Article 6 - the lawfulness of data processing.

4. Personal Data Processing without Data Subject's Consent. The following case depicts the mentioned violation. EDP Comercializadora, S.A.U. was fined EUR 75.000 by Spanish Data Protection Authority because it processed personal data in connection with a gas contract without the consent of the applicant. [16]The decision finds that the applicant received an invoice for a gas contract which he did not sign and that EDP Comercializadora claims that the applicant is a party to a contract with another energy company which has a supply contract with EDP Comercializadora and that the processing of data is therefore justified. However,

---

[14] Il Garante per la protezione dei dati personali

https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9244365 (last accessed March 2020)

[15]Besluit tot het opleggen van een bestuurlijke boete
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_knltb.pdf (last accessed March 2020)

[16]Case of EDP Comercializadora, S.A.U. https://www.aepd.es/es/documento/ps-00025-2019.pdf (last accessed March 2020)

40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

this was found to violate the GDPR, because the reason EDP Comercializadora brought did not comply with any basis of lawfulness of data processing described in Article 6.

5. Obtaining Consent of a Data Subject through its inactivity. A display of such a violation can be the case of Spanish Data Protection Authority v HM Hopitales[17]. Here the data subject stated that at the time of his admission to hospital he had to fill in a form containing a checkbox indicating that, if he did not tick it, he agreed to the transfer of his data to third parties. This form, provided by HM, was not compatible with the GDPR, since consent was to be obtained through the activity of the data subject rather than inactivity.

6. Obtaining more information than is necessary for the purpose

The fine was imposed by Austrian Data Protection Agency against a private person who was using CCTV at his home.[18] The video surveillance covered areas which were intended for the general use of the residents of the multi-party residential complex, namely: parking lots, sidewalks, courtyard, garden and access areas to the residential complex; in addition, the video surveillance covered garden areas of an adjacent property. Video surveillance was therefore found to be not proportionate to the purpose and not limited to what is necessary. This case was found to violate Article 5.1 (a) and (c) GDPR, Article 6.1 and Article 13, which states that information should be provided to data subjects, where personal information is being collected.

7. Insufficient legal basis for data processing can also be found in cases where GDPR **article 9('special categories of personal data'** see footnote for explanation**)[19]** is violated. The cases below show violation of article 9 of the GDPR:

- In the case of Swedish school Skellefteå[20], which tried to use facial recognition technology to monitor the attendance of students. Even though, in general, data

[17]Case of HM Hopitale https://www.aepd.es/es/documento/ps-00187-2019.pdf

[18]Unlawful CCTV Usage Case https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181220_DSB_D550_037_0003_DSB_2018_00/DSBT_20181220_DSB_D550_037_0003_DSB_2018_00.pdf (last accessed March 2020)

[19]**Article 9** of the GDPR states: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

[20] Case of Swedish School https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf (last accessed March 2020)

40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

processing for the purpose of monitoring attendance is possible, it was found that doing so with facial recognition is disproportionate to the goal to monitor attendance.

- A school in Gdansk used bio-metric fingerprint scanners to authenticate students for the payment process in the school canteen.[21] Although the parents had given their written consent to such data processing, the data protection authority considered the processing of the student data to be unlawful, as the consent to data processing was not given voluntarily.

8. Another basis that is among common violations by data controllers is insufficient technical and organizational measures to ensure information security

Insufficient technical and organizational measures to ensure information security violates article 32 of GDPR concerning security of data processing.

Article 32.1 states:

"... [T]he controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymization and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing."

The cases below show, how in practice data controllers violate the respective article:

- The Federal Commissioner for Data Protection and Freedom of Information (BfDI) in Germany has fined telecommunications service provider 1 & 1 Telecom GmbH a fine of EUR 9,550,000, because the company had not taken sufficient technical and organizational measures to prevent unauthorized persons from receiving information about customer data from customer service by telephone.[22]

[21] Gdansk School Case https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018 (last accessed March 2020)

[22] 1&1 Telecom GmbH Case https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverh%C3%A4ngtGeldbu%C3%9Fe1u1.html (last accessed March 2020)

40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

- Bulgaria's National Revenue Agency in its capacity as data controller did not implement appropriate technical and organizational measures.[23] As a result personal data of the State's citizen's was subject to unauthorized access, in particular, names, personal identification numbers and addresses of Bulgarian citizens, telephone numbers, e-mail addresses and other contact information, data from annual tax returns of individuals, data from records of income paid to individuals, data from social security declarations, data for health insurance contributions were subject to unauthorized disclosure and dissemination.
- The Information Commissioner (ICO) issued a notice of its intention to fine British Airways GBP 183.39 million for breach of article 32.[24] The User traffic to the British Airways website was diverted to a fraudulent site, which harvested customer details. Personal data of approximately 500.000 customers were compromised in the accident.

9. Non-compliance with general data protection principles is another basis of common violations of the GDPR.

Non-compliance with general data protection principles arises mainly in violation of article 5 of the GDPR. Example cases:

- Deutsche Wohnen was found liable in infringement of GDPR articles 5 and 25(data protection by design and default) and was fined 14,5 million euros. [25]It used an archiving system for the storage of personal data of tenants that did not provide for the possibility of removing data that was no longer required. Personal data of tenants were stored without checking whether storage was permissible or even necessary. It was therefore possible to access personal data of affected tenants which had been stored for years without this data still serving the purpose of its original collection. This involved data on the personal and financial circumstances of tenants, such as salary statements, self-disclosure forms, extracts from employment and training contracts, tax, social security and health insurance data as well as bank statements.

[23] Bulgarias National Revenue Agency Case https://www.cpdp.bg/index.php?p=news_view&aid=1519 (last accessed March 2020)
[24] British Airways Case https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ (last accessed March 2020)
[25] Deutsche Wohnen Case https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf (last accessed March 2020)

40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia law@aua.am

- A fine was imposed on Danish company IDdesign as a result of an inspection carried out in autumn of 2018 because article 5 infringement was found.[26] IDdesign had processed personal data of approximately 385,000 customers for a longer period than necessary for the purposes for which they were processed. Additionally, the company had not established and documented deadlines for deletion of personal data in their new CRM system. The deadlines set for the old system were not deleted after the deadline for the information had been reached. Also, the controller had not adequately documented its personal data deletion procedures.
- Hellenic Data Protection Authority (HDPA) fined for EUR200,000 the Telecommunication Service Provider Company for violation of article 5 (1) c, and article 25 of th GDPR.[27] A large number of customers were subject to telemarketing calls, although they had declared an opt-out for this. This was ignored due to technical errors.

10. The next common violation of the GDPR according to the statistics is the insufficient fulfillment of data subjects' rights.

This violation arises when one of the fundamental rights of a data subject are disconcerned. Under the GDPR the fundamental rights of data subjects are:

1. Right to Information (article 12) - provides the data subject with the ability to ask a company for information about what personal data (about him or her) is being processed and the rationale for such processing.

The following example shows how it is used in practice. The Belgian "Nursing Care Organization" was found to infringe articles 12, 15 and 17 of the GDPR by failing to act on requests from the data subject to get access to his data and to have his data erased. [28]

2. Right to Access (article 15) - provides the data subject with the ability to get access to his or her personal data that is being processed. This request provides the right for data subjects to see or view their own personal data, as well as to request copies of the personal data.

---

[26]IDesign Case https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/jun/tilsyn-med-iddesigns-behandling-af-personoplysninger/ (last accessed March 2020)

[27] Tellecommunications Sevice Case www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=3,241,32,146,79,143,149,112 (last accessed March 2020)

[28]Nursing Care Organization case https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/DEQF_13-2019_FR_ANO.pdf (last accessed March 2020)

40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

As an example, Bulgarian Commission for Personal Data Protection fined a company for not timely and in complete way answering to the request of the employee for access to his personal data[29]

Another example of the violation of right to access was found in the following case. Portuguese Data Protection Authority fined a company for EUR 20.000 for the denial of the right to access recorded phone calls by the Data Subject. [30]

A violation of article 15 was found in the Cyprus case. The Office of the Commissioner for Personal Data Protection of Cyprus imposed a penalty on State Hospital for latter not being able to provide the access to personal medical files to the patient, because they were lost.[31]

3. Right to erasure or 'right to be forgotten' (article 17) - provides the data subject with the ability to ask for the deletion of their data.

The Swedish data protection authority has fined Google LLC €7 million for failing to adequately comply with its obligations regarding the right of data subjects to have search results removed from the results list. This violated articles 5, 6 and 17 of GDPR.[32]

4. Right to object (article 21) - provides the data subject with the ability to object to the processing of their personal data.

German Company Hamburger Volksbank was found to violate article 21 of GDPR while sending a customer a newsletter with advertising content by e-mail, although this customer had previously expressly objected to the sending of further advertising letters.[33]

---

[29]Bulgarian Employee case https://www.cpdp.bg/?p=element_view&aid=2177 (last accessed March 2020)
[30]Portuguese Company case https://www.cnpd.pt/home/decisoes/Delib/DEL_2019_21.pdf (last accessed March 2020)

[31] Cyprus State Hospital case https://www.agplaw.com/cyprus-gdpr-commissioner-fines-newspaper-and-hospital/ (last accessed March 2020)
[32] Google LLC case https://www.datainspektionen.se/globalassets/dokument/beslut/2020-03-11-beslut-google.pdf (last accessed March 2020)
[33] Hamburger Volksbank case https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf (last accessed March 2020)

40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia law@aua.am

Insufficient fulfillment of information obligation is next type of common violation according to the statistics.

This violation arises mainly due to infringement of article 13 of the GDPR. **Article 13** states that information is to be provided where personal data are collected from the data subject.

We want to bring up three cases which showcase the violation of article 13:

- Spanish company Solo Embrague did not present a privacy policy or a cookie banner on its main page on the corporate website. [34]
- The sanctions were applied to the UTTIS INDUSTRIES SRL Romanian company because it could not prove that the data subjects were informed about the processing of personal data / images through the video surveillance system, which they have been operating since 2016.[35]
- Portugal company was fined for nonexistence of signalization regarding the use of CCTV systems [36]
- Austrian Betting Place Video surveillance was not sufficiently marked and a large part of the sidewalk of the facility was recorded. Surveillance of the public space in this way, i.e. on a large scale by private individuals, is not permitted.[37]

Insufficient fulfillment of data breach notification obligations

This infringement arises mainly from article 33 violation. **Article 33.1** states: "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the

[34] Solo Embrague case https://www.aepd.es/es/documento/ps-00469-2019.pdf (last accessed March 2020)
[35] Utties Industries SLL case https://www.dataprotection.ro/?page=A_patra_amenda&lang=ro (last accessed March 2020)
[36] Portugal CCTV case https://www.cnpd.pt/home/decisoes/Delib/DEL_2019_222.pdf (last accessed March 2020)
[37] Austrian Betting Place Case https://www.dsb.gv.at/documents/22758/116802/Straferkenntnis+DSB-D550.038+0003-DSB+2018.pdf/fb0bb313-8651-44ac-a713-c286d83e3f19 (last accessed March 2020)

40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia law@aua.am

notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

The cases illustrate how insufficient fulfillment of data breach notification can lead to liability:

- On July 6, 2018, HVV GmbH was informed by a customer about a security gap on the website www.hvv.de, which was caused by an update on February 5, 2018 and concerned the so-called Customer E-Service (CES). The security gap consisted in the fact that customers logged in to the CES who had an HVV Card and linked their CES customer account to at least one active contractual relationship in background systems could, by changing the URL, display data of other customers who had an HVV Card. This data breach was not reported to the data protection authority in a timely manner. [38]

- Hungarian military hospital did not meet the reporting deadline for data breaches. Another part of the fine relates to a lack of technical and organizational measures.[39]

- The data controller did not fulfill its data breach notification obligations when a flash memory with personal data was lost.[40]

Insufficient Cooperation with supervisory authority breaches articles 31 ('Cooperation with supervisory authority') and article 58 ('powers'). **Article 31** states that a cooperation should take place with supervisory authority, while **article 58** describes investigation, corrective, authorization and advisory powers of the supervisory authority. Few cases available arose when the companies didn't cooperate, or didn't comply in the timely manner. The fines varied from EUR 511 to EUR 8000.

Insufficient data processing agreement breaches **article 28.3** of the GDPR, which stipulates "Processing by a processor shall be **governed by a contract** or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of

[38] Non-timely reporting of data breach https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf (last accessed March 2020)
[39]Hungarian military hospital case https://www.naih.hu/files/NAIH-2019-2485-hatarozat.pdf (last accessed March 2020)
[40]Flash memory case https://www.naih.hu/files/NAIH-2019-2471-hatarozat.pdf (last accessed March 2020)

40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia law@aua.am

personal data and categories of data subjects and the obligations and rights of the controller." Currently only 2 such cases exist with fines EUR 5000 and EUR 9380.

Lack of appointment of data protection officer infringes GDPR **article 37** ('designation of data protection officer'). One of two cases currently available concernd Facebook Germany GmbH with fine of EUR 51.000, where Facebook acted negligently and did not violate the duty to appoint a data protection officer but only the notification obligation.[41]

To conclude, in this chapter the most common GDPR violations which result in huge fines were analyzed using case-study methodology. Based on this analysis we can construct a privacy policy which can aid IT companies to avoid such violations.

[41]Facebook Germany case https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf (last accessed March 2020)

40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

CHAPTER 2

The Methods to Avoid Liability

In this chapter, we show how the drawbacks identified in the previous chapter can be addressed. As we can conclude from chapter 1, the general principle of privacy policies should be the protection of data subject's privacy above everything, that is to say privacy of data subjects by design and default. The term "privacy by design" is a concept developed by Information and Privacy Commissioner of Ontario, Canada Ann Cavoukian. In this concept privacy by design can be broken down into "7 foundational principles[42]":

1. Proactive not Reactive, Preventative not Remedial;
2. Privacy as the Default Setting;
3. Privacy Embedded into Design;
4. Full Functionality —Positive-Sum, not Zero-Sum;
5. End-to-End Security —Full Lifecycle Protection;
6. Visibility and Transparency —Keep it Open;
7. Respect for User Privacy —Keep it User-Centric.

She emphasised the need to be proactive in considering the privacy requirements as of the design phase throughout the entire data lifecycle, to be "embedded into the design and architecture of IT systems and business practices...without diminishing functionality...", with privacy as the default settings, end-to-end security including secure data destruction and strong transparency subject to independent verification. The principle of privacy by default involves "ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy —it is built into the system, by default". This statement can be used as an operational definition of the principle of privacy by default, where the individual does not bear the responsibility for his or her personal data protection when using a service but enjoys "automatically" (no need for active behaviour) the fundamental right of privacy and personal data protection. Based on this principle, **Article 25** of the GDPR, called "Data protection by design and by default", provides that the controller must implement appropriate technical and organisational measures, both at the design phase

[42] Ann Cavoukian "7 foundational principles of privacy by Design" https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf (last accessed March 2020)

40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

of the processing and at its operation, to effectively integrate the data protection safeguards to comply with the Regulation and protect the fundamental rights of the individuals whose data are processed. Those measures shall be identified taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing as well as the risks for the rights and freedoms of those individuals. The Article states that, by default, only personal data that are necessary for each specific purpose of the processing may be processed.

In addition, a GDPR-compliant privacy-policy should also contain the following information:

1. **Who are the processing entities** – who collect personal information and who uses that information.
2. **Who are if any the third-parties** - The policy must state the sources of data, and with whom the collected data is shared. If the data is going to be shared with third-parties, GDPR requires specifying who the third parties are, and for what purpose they would use this data. We also need to consider international transfers of personal data. **Articles 44 – 50**[43] describe how the transfer should be done. The transfer should be done only if the other receiving country's company has a contract with the sender that contains standard data protection clauses, or is based in a country, that is included in the list of countries ensuring the same level of privacy protection and are considered safe for such transfers.
3. **Data Categories** - what personally identifiable data is collected (requirement of Articles 14, 20). The controller must clearly state the attributes of personal data (name, email, phone number, IP, etc.) being collected.
4. **User Controls -** how can the user request the following
    1. (a) All the personal data associated with the user along with its source, purpose, the list of third-parties to which it has been shared etc. (Article 15)
    2. (b) Raise objection to the use of any attribute of their personal data (Article 21)
    3. (c) Personal data to be deleted without any undue delay (Article 17)
    4. (d) Personal data to be transferred to a different controller (Article 20)

[43] Articles 44-50 of the GDPR https://gdpr-info.eu/chapter-5/ (last accessed March 2020)

40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

5. **Policy Updates –** notification of users when changes are made to the privacy policy (Article 14).
6. **Retention -** when will the collected data expire and be deleted (Articles 5(1)(e), 13, 17).

We have identified the basic requirements that the GDPR sets for a Prvicay policy to be considered compliant with the regulation and safe for data subjects. To construct an effective privacy policy let us summarize the most common GDPR violations from chapter 1. Principles of data protection that are mostly violated are:

1. Transparency: The data subject should be made aware of who has their data and how it is being processed. Data Transfer to third-parties should be done through consent of the data subject, and the identity of third parties should be explicitly mentioned.

2. Consent: The data subject should give explicit consent for the collection and processing of their data. The consent should not be obtained through data subject's inactivity.

3. Processing Control: The data subject should have control over what types of processing are applied to their data. He or she should be able to obtain a copy of any data related to them. The data should be deleted by the data subject's request.

4. Purpose Limitation: The data collected about the subject should be processed only for the purpose mentioned in policy. The information should be collected only to the extent necessary for the purpose and processed no longer than necessary for the purpose.

5. Data Protection: The data processor should implement appropriate technical and organizational measures to ensure a level of security of information.

6. Data Processing Agreement: Data processing should be governed by a contract, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

All the principles described above represent the design criteria for our privacy policy template. Based on them, we can conclude, that GDPR-compliant Privacy Policy must include the following topics:

- **Introduction to company**

40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

The Privacy Policy should start with a brief explanation of the company and include the date from which it takes effect – the effective date. It should include the legal name and business address of the company.

- **Data that is collected**

  The policy should specify what kind of data is being collected.

- **Purpose of data collection**

  The exact purpose of why the data is collected should be specified.

- **Lawful basis of data collection**

  If relying on "legitimate interests," of data processing, the policy should specify what are legitimate interests. If “consent” is used as a legal basis, than the policy should include a part where the user has a right to withdraw the consent.

- **How and for how long the data is stored**

  The Privacy Policy needs to give details of how long the personal data collected will be stored. It may be determined by the length of time for which the data is needed.

- **Data subject’s rights**

  Data subject’s rights has to be included in the Privacy Policy

- **Who the data is shared with**

  Policy needs to provide details about the third-parties the company is going to share data subject’s personal data with.

- **Changes to Privacy Policy**

  Data subjects must be notified about any changes to Privacy Policy. The means of notifications should be described in policy (via email, regular mail, call).

- **Contact details**

  If the company has a Data Protection Officer (DPO) and/or EU Representative, their contact details should also be included.

Under **Article 12** of the GDPR the Privacy Policy must be “… in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.” Therefore avoiding usage of legal terminology where possible will generally be a good practice.

40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

Based on what we have discussed, here you can find a sample of Privacy Policy:

Sample Privacy Policy

Effective date: April 1st, 2020.

Company Name is committed to ….

This Privacy Policy applies to Company Name…. The Company is owned and operated by … (Owner's Legal Name), with its principal place of business at ….(address.)

Our Company Collects the following data:

- Personal Data you provide to us
- Personal Data we collect automatically
- If sensitive data is to be collected and processed it should be necessarily mentioned
- If data on minors is to be processed should be mentioned, if not, it is necessary to mention that the company is not processing data on minors

Our Principles of Regarding user Privacy and Protection

- We only collect and process data when it is absolutely necessary and keep it only as long as it is necessary for providing you with our services
- We never share personal information with anyone else without your permission

How the personal data is being used:

- Verification of your identity
- …..

Lawful basis of data collection:

40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

Purpose/Activity	**Type of data**	**Lawful basis for processing including basis of legitimate interest**
To register you as a new customer	(a) Identity (b) Contact	Performance of a contract with you
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b)Asking you to leave a review or take a survey	(a) Identity (b) Contact (c) Profile (d)Marketing and Communications	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)
To use data analytics to improve our products/services, marketing, customer relationships and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to develop our business and to inform our marketing strategy)

How long will we keep your personal information:

Your personal data will not be kept for longer than is necessary to fulfill the specific purposes outlined in this Privacy Policy, and to allow us to comply with legal requirements. Any data

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
law@aua.am

we hold will be kept anonymous. Any personally identifiable information, such as your name, address, date of birth and telephone number will be deleted after a defined period. ….

Your rights:

- Request access for your personal information
- Request erasure of your personal information
- Request correction of your personal information

Changes to Privacy Policy:

The privacy policy may be changed time to time. When this happens we will notify you by email.

Also, DPO details to be contacted to exercise the mentioned rights

40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

CONCLUSION

The big data revolution has triggered an explosion in the collection and processing of our personal data, leading to numerous societal benefits. At the same time, this trend of ever-increasing data collection raises new concerns about data privacy. The prevalence of data breaches indicates that these concerns are well-founded. With the arrival of the European Union's General Data Protection Regulation (GDPR), several companies are making significant changes to their systems to achieve compliance. It imposes huge fines up to 20 million EUR for breaches of its regulations. Therefore, non-compliance with data privacy regulations is costly or impossible for many organizations.

Since Privacy policy is the main medium of information dissemination between the data controller and the users, in this paper we try to come up with an effective template of privacy policy which can be used for IT companies to escape liability. First, the paper analyzes the GDPR breach cases to establish most common reasons of GDPR violations. Those breaches were insufficient legal basis for data processing, insufficient technical and organizational measures to ensure information security, non-compliance with general data processing principles, insufficient fulfillment of data subjects rights, insufficient fulfillment of information obligations, insufficient fulfillment of data breach notification obligations, insufficient cooperation with supervisory authority, insufficient data processing agreement and lack of appointment of data protection officer. Based on this analysis, we also discussed other requirements that GDPR sets for the Privacy Policy. We found out that Privacy by design and default is a major requirement for the companies to meet at the phase of designing the system. On top of that, there is another requirement of data processing transparency, data subject's consent and processing control and purpose limitation when data processing is required. Based on our study, we propose an effective privacy policy template which can be used by the IT companies. This privacy policy would allow the IT companies to escape the common violations and would provide them a legal shield against possible litigation.

40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

BIBLIOGRAPHY

Legal Instruments

General Data Protection Regulation (GDPR)

ՏԵՂԵԿԱՏՎԱԿԱՆ ՏԵԽՆՈԼՈԳԻԱՆԵՐԻ ՈԼՈՐՏԻ ՊԵՏԱԿԱՆ ԱՋԱԿՑՈՒԹՅԱՆ ՄԱՍԻՆ", available at https://www.arlis.am/DocumentView.aspx?docID=95017 (last accessed March 2020)

Electronic Publications

Ann Cavoukian "7 foundational principles of privacy by Design" https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf (last accessed March 2020)

GDPR fines. https://www.dlapiper.com/en/ireland/insights/publications/2020/01/gdpr-data-breach-survey-2020/ (last accessed February 2020)

GDPR penalties and fines. https://www.itgovernance.co.uk/dpa-and-gdpr-penalties (last accessed March 2020)

DLA Piper. (2005, January 26). Retrieved from https://en.wikipedia.org/wiki/DLA_Piper#cite_note-facts-1

Flavián, C., Guinalíu, M.: Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. Ind. Manag. Data Syst. 106(5), 601– 620 (2006)

Make Armenia a country of Modern technologies: President meets representatives of IT companies. https://en.armradio.am/2020/02/07/make-armenia-a-country-of-modern-technologies-president-meets-representatives-of-it-companies/ (last accessed February 2020)

Microsoft privacy policy https://privacy.microsoft.com/en-us/privacystatement?PrintView=true (last accessed February 2020).

40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

Statistics of the fines by the types of violations https://www.enforcementtracker.com/?insights (last accessed March 2020)

Mohan, J., Wasserman, M., & Chidambaram, V. (2019). Analyzing GDPR Compliance Through the Lens of Privacy Policy. Heterogeneous Data Management, Polystores, and Analytics for Healthcare, 82-95. doi:10.1007/978-3-030-33752-0_6

Obar, Jonathan A. and Oeldorf-Hirsch, Anne, The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services (June 1, 2018). TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy, 2016.. Available at SSRN: https://ssrn.com/abstract=2757465 or http://dx.doi.org/10.2139/ssrn.2757465

Cases

Austrian Betting Place Case https://www.dsb.gv.at/documents/22758/116802/Straferkenntnis+DSB-D550.038+0003-DSB+2018.pdf/fb0bb313-8651-44ac-a713-c286d83e3f19 (last accessed March 2020)

Besluit tot het opleggen van een bestuurlijke boete https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_knltb.pdf (last accessed March 2020)

British Airways Case https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ (last accessed March 2020)

Bulgaria's National Revenue Agency Case https://www.cpdp.bg/index.php?p=news_view&aid=1519 (last accessed March 2020)

Bulgarian Employee case https://www.cpdp.bg/?p=element_view&aid=2177 (last accessed March 2020)

Case of Swedish School https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf (last accessed March 2020)

40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

Case of EDP Comercializadora, S.A.U. https://www.aepd.es/es/documento/ps-00025-2019.pdf (last accessed March 2020)

Case of HM Hopitale https://www.aepd.es/es/documento/ps-00187-2019.pdf (last accessed March 2020)

Cyprus State Hospital case https://www.agplaw.com/cyprus-gdpr-commissioner-fines-newspaper-and-hospital/ (last accessed March 2020)

Datenschutzskandal: Millionenstrafe für Post https://wien.orf.at/stories/3019396/ (last accessed on March 2020).

Deutsche Wohnen Case https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf (last accessed March 2020)

Facebook Germany case https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf (last accessed March 2020)

Flash memory case https://www.naih.hu/files/NAIH-2019-2471-hatarozat.pdf (last accessed March 2020)

Gdansk School Case https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018 (last accessed March 2020)

Google LLC case https://www.datainspektionen.se/globalassets/dokument/beslut/2020-03-11-beslut-google.pdf (last accessed March 2020)

Hamburger Volksbank case https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf (last accessed March 2020)

Hungarian military hospital case https://www.naih.hu/files/NAIH-2019-2485-hatarozat.pdf (last accessed March 2020)

40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

IDesign Case
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/jun/tilsyn-med-iddesigns-behandling-af-personoplysninger/ (last accessed March 2020)

Il Garante per la protezione dei dati personali
https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9244365 (last accessed March 2020)

Non-timely reporting of data breach
https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf (last accessed March 2020)

Nursing Care Organization case
https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/DEQF_13-2019_FR_ANO.pdf (last accessed March 2020)

Portugal CCTV case https://www.cnpd.pt/home/decisoes/Delib/DEL_2019_222.pdf (last accessed March 2020)

Portuguese Company case https://www.cnpd.pt/home/decisoes/Delib/DEL_2019_21.pdf (last accessed March 2020)

Solo Embrague case https://www.aepd.es/es/documento/ps-00469-2019.pdf (last accessed March 2020)

Tellecommunications Sevice Case
www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=3,241,32,146,79,143,149,112 (last accessed March 2020)

Unlawful CCTV Usage Case
https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181220_DSB_D550_037_0003_DSB_2018_00/DSBT_20181220_DSB_D550_037_0003_DSB_2018_00.pdf (last accessed March 2020)

Utties Industries SLL case https://www.dataprotection.ro/?page=A_patra_amenda&lang=ro (last accessed March 2020)

40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

1&1 Telecom GmbH Case

https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverh%C3%A4ngtGeldbu%C3%9Fe1u1.html (last accessed March 2020)

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
law@aua.am