**Good (16)**

1[0]: Concept: Enforceable data subject rights

Question: Were the data subjects informed about their rights regarding their personal data?

Context:It also appeared that the company's files contained several excessive comments related to customers or their health conditions. In addition, people were not properly informed about the processing of their personal data, or about the recording of the conversations they had with the company. In total, following its investigations the CNIL found five breaches of the GDPR: -         Violation of the right to object, Article 21(2) GDPR: no procedure was implemented to ensure effectively that persons who opposed telephone solicitation were no longer called); -         Violation of the principle of data minimization, Article 5(1)(c) GDPR: inadequate and offensive comments or irrelevant comments related to people's health were found in the company's customer file; -         Violation of Articles 12 and 13 GDPR: insufficient information on the processing of data subject’s personal data and their rights; -         Violation of Articles 46 and 49 GDPR:  the controller did not provide appropriate safeguards for data subjects; -         Failure to cooperate with the CNIL, Article 31 GDPR.

Answer: people were not properly informed

1[2]: Concept: Enforceable data subject rights

Question: Were the data subjects informed about their rights regarding their personal data?

Context:The HDPA identified deficiencies as follows: first of all, the HDPA found that the Ministry never made a detailed investigation on the lawfulness of the processing purposes under [[Article 6 GDPR#4|Article 6(4) GDPR]], in particular with regard to the consent for access to information stored in a user's terminal equipment, when is not necessary to provide the service requested by the user. Regarding the principle of transparency and the right to access by the data subject, according to Article 12 and 14 GDPR, the information provided by the Ministry to the data subjects was not considered appropriate and sufficient. The HDPA found in particular that the provided information was not easy to understand and (lack of accessibility and of clear and simple wording), especially vis-à-vis children.

Answer: the information provided by the Ministry to the data subjects was not considered appropriate and sufficient

1[3]: same as 1[0]

1[4]: Concept: Enforceable data subject rights

Question: Were the data subjects informed about their rights regarding their personal data?

Context:The AEPD also evaluated the position of the three entities involved in the case, and held that according to the processing agreements that were in place, Amazon Road was the controller responsible for the processing carried out by Amazon India and Accurate Background, and that because these processors were located outside the EEA (in India and the United States respectively), international data transfers were taking place. The AEPD found that, in this case, data subjects' consent to data transfers would not be valid in accordance with [[Article 49 GDPR|Article 49(1) GDPR]] and [[Article 7 GDPR]], given that consent was required within the contract without an option to refuse, it was not explicit, and no information was given to the data subject regarding the risks of these data transfers. However, the AEPD found that the data transfers were lawful according to [[Article 46 GDPR]], since the SCCs in Amazon's processing agreements included appropriate technical and organisational data protection measures, and Accurate Background was adhered to the EU-US Privacy Shield during the time that the data transfers took place.

Answer: consent was required within the contract without an option to refuse, it was not explicit, and no

2[0]: Concept: Enforceable data subject rights

Question: Has the organization provided a direct avenue for data subjects to enforce their rights?

Context:These law allow for bulk collection of personal data. They do not allow a data subject to enforce any rights before a tribunal. ''With regard to national law relating to collection and processing of data:'' The French Court outlined that Article L. 1462-1 of the public health code provides for the Health Data Hub and the collection of health data from the existing national health data system (as per Article L. 1461-1).

Answer: They do not allow a data subject to enforce any rights before a tribunal

2[1]: Concept: Enforceable data subject rights

Question: Has the organization provided a direct avenue for data subjects to enforce their rights?

Context:The DPA remarks that, according the Schrems II Judgment, the transfer of data to the United States may result in violations of fundamental rights, given that the US legislation allows for access to the data because of national security and public interest reasons. Such inferences are not reasonable, as limitations to fundamental rights are not clearly defined; as there are no clear and precise rules on the application of such measures or minimum requirements to protect against risks of abuse; there is no requirement for a necessity test; and there are no enforceable rights for data subjects or legal remedies. The Portuguese DPA found that the National Institute had not undertaken a sufficient Data Protection Impact Assessment, had not consulted the supervisory authority prior to processing, and had therefore not adopted adequate additional safeguards before using the services of a data processor who was headquartered in the United States.

Answer: there are no enforceable rights for data subjects or legal remedies

6[0]: Concept: Effective legal remedies for data subjects

Question: Are there established procedures within the organization for data subjects to seek legal remedies?

Context:The parties still agreed supplementary measures. First, Google has established policies and procedures and a team of qualified lawyers for handling authority requests for user data. Second, Google offers and the controller implemented the Anonymize IP feature and, finally, the controller had applied a redaction script on the website to prevent personal data unintentionally being shared with Google.

Answer: Google has established policies and procedures and a team of qualified lawyers for handling authority requests for user

11[0]: Concept: Legally binding and enforceable instrument

Question: Does the instrument in question meet the criteria for being legally binding under relevant laws?

Context:In its privacy policy the controller simply informed consumers about data transfers to third parties and countries, without any further legal effect. This document did not constitute a legally binding contract offered to customers by the controller, as the Consumer Center suggested. The court also held that the Consumer Center's claim with regard to the cookie banners was unfounded.

Answer: not

21[0]: Concept: Standard data protection clauses

Question: Has the organization implemented Standard Contractual Clauses (SCCs) for data transfers?

Context:The Norwegian DPA then proceeded to investigate the case and notified the controller asking for information about the investigated facts. In response, the controller stated that after becoming aware of the judgment in the Schrems II case, it reassessed its contract with Google, the processor, and adopted standard contractual clauses (SCCs) as the legal basis for the transfer of data to the US. Furthermore, it claimed that it was taking additional measures to ensure the protection of personal data transferred outside the EU/EEA.

Answer: adopted standard contractual clauses (SCCs) as the legal basis for the transfer of data

21[1]: Concept: Standard data protection clauses

Question: Has the organization implemented Standard Contractual Clauses (SCCs) for data transfers?

Context:According to the website provider and Google LLC, the website controller qualifies as controller ([[Article 4 GDPR#7|Article 4(7) GDPR]]) and Google LLC as processor ([[Article 4 GDPR#8|Article 4(8) GDPR]]) for data processing in connection with Google Analytics. Furthermore, according to the privacy documents provided on the website or included via hyperlink, the website provider and Google LLC entered into standard contractual clauses under [[Article 46 GDPR#2#c|Article 46(2)(c) GDPR]] ([https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32010D0087 Commission Decision2010/87 of 05.02.2010]; SCCs) as a mechanism for transfers of personal data with regard to Google Analytics. On 18.08.2020, the data subject (represented by ''noyb'') filed a complaint with the DSB against both the website provider (in its role as data exporter) and Google LLC (in its role as data importer), arguing that both respondents violated Articles 44 et. seqq.

Answer: the website provider and Google LLC entered into standard contractual clauses under [[Article 46

21[2]: Concept: Standard data protection clauses

Question: Has the organization implemented Standard Contractual Clauses (SCCs) for data transfers?

Context:They found this to apply to their use of Google Analytics since the agreement was with Google as a US processor of their. With the Privacy Shield now invalidated, the controller entered into standard contractual clauses (SCCs) Module Two with Google on 12 August 2020 for data transfers to the US. However, the controller did not carry out a thorough review of potential third country legislation (a "transfer impact assessment"), as it, according to information from Google, was not possible to determine the exact location of processing.

Answer: the controller entered into standard contractual clauses (SCCs) Module Two with Google on 12

21[3]: Concept: Standard data protection clauses

Question: Has the organization implemented Standard Contractual Clauses (SCCs) for data transfers?

Context:This general consent clause also stated that it would exonerate Amazon of any responsibility, damages claims, or other charges related to the processing and transfer of data as far as the law permits it. Amazon Road established an Intra-Group Data Transfer and Processing Agreement with Amazon India and a Data Processing Agreement with Accurate Background, which both included Standard Contractual Clauses (SCCs) with technical and organisational measures required for data processing. Additionally, Accurate Background was adhered to the EU-US Privacy Shield transatlantic data transfer framework.

Answer: both included Standard Contractual Clauses (SCCs) with technical and organisational measures

21[4]: similar to 21[1]

21[5]: Concept: Standard data protection clauses

Question: Has the organization implemented Standard Contractual Clauses (SCCs) for data transfers?

Context:Meta Ireland had been transferring personal data to the U.S. despite the lack of a valid adequacy decision under [[Article 45 GDPR]] (as both “safe harbor” and its successor “privacy shield” were invalidated by the CJEU in Schrems I and II). While negotiation of a new adequacy decision for EU-U.S. data transfers are ongoing, Meta Ireland claimed to have undertaken data transfers on the basis of standard contractual clauses adopted by the Commission under [[Article 46 GDPR#2c|Article 46(2)(c) GDPR]] even before the CJEU passed the Schrems II decision. First, the Irish DPA ascertained whether US law guaranteed an essentially equivalent level of protection of data protection rights in light of Schrems II.

Answer: adopted by the Commission

25[0]: Concept: Standard data protection clauses

Question: Are there mechanisms in place to review and update the standard data protection clauses in response to legal or operational changes?

Context:After establishing this, the Court emphasized that the validity of the SCCs, however, did depend on whether there were effective mechanisms in place that make it possible to ensure compliance with the level of protection required by EU law. Important to note is that here the Court held that the SCCs in themselves did provide for such mechanisms. However, it went on to stress that where these mechanisms cannot be complied with, the transfers of personal data pursuant to these clauses is to be suspended or prohibited.

Answer: effective mechanisms in place

39[0]: Concept: Competent supervisory authority

Question: Has the competent supervisory authority ever mandated corrective actions for the organization?

Context:In other words, the fact that the controller claimed to have no knowledge whether data were transferred to the US by Meta Ireland showed that the controller disregarded its responsibilities under the GDPR. In light of the above, the Danish DPA reprimanded the controller and ordered it to bring its processing activities in compliance with [[Article 25 GDPR|Article 25]], [[Article 5 GDPR|5]] and [[Article 24 GDPR|24 GDPR]]. within a month.

Answer: the Danish DPA reprimanded the controller and ordered it to bring its processing

42[1]: Concept: Contractual clauses

Question: Are these contractual clauses in compliance with the requirements of relevant data protection laws?

Context:The Municipality, in its capacity as the controller, instructed its processor (Google Ireland) to transfer personal data to a sub-processor (Google LLC) in the United States. The transfer was based on standard data protection clauses pursuant to [[Article 46 GDPR|Article 46(2)(c) GDPR]]. In C-311/18, Schrems II, the CJEU clarified that the use of SCCs does not always constitute "an adequate means of ensuring the effective protection of the personal data transferred to the third country in question in practice.

Answer: not always constitute "an adequate means of ensuring the effective protection of the personal data transferred to

42[3]: Concept: Contractual clauses

Question: Are these contractual clauses in compliance with the requirements of relevant data protection laws?

Context:It considered whether the respondent could rely on any transfer mechanisms under Chapter V. of the GDPR and held: \* The respondent could not rely on an adequacy decision following [[CJEU - C-311/18 - Schrems II|C-311/18]]. \* The SCCs concluded between the respondent and Google LLC do not offer an adequate level of protection, because: \*\* Google LLC qualifies as an "''electronic communication service provider''" under 50 U.S. Code § 1881(b)(4) and is subject to surveillance by US intelligence services, and \*\* any contractual, organisational and technical measures which Google put into place to complement the SCCs were insufficient as they could not prevent US intelligence services from accessing the data subject's personal data \*\* Notably, the CNIL rejected Google's argument that any Google Analytics data were pseudonymised, highlighting that Universal Unique Identifiers do not meet the definition of pseudonymisation under [[Article 4 GDPR#5|Article 4(5) GDPR]], as their sole purpose is to identify users. \*

Answer: The SCCs concluded between the respondent and Google LLC do not offer an adequate level of

**Bad (13)**

1[1]: Concept: Enforceable data subject rights

Question: Were the data subjects informed about their rights regarding their personal data?

Context:It was therefore necessary for the international agreement, as the legal basis for the transfer, to include appropriate data protection safeguards under [[Article 46 GDPR|Article 46(2)(a) GDPR]]. In this case, the DPA found that the agreement contained no definition of data protection, no retention period, no mention of the rights of data subjects and no mention of appeal mechanisms. The DPA therefore concluded that the Belgian tax authority could not rely on [[Article 96 GDPR|Article 96 GDPR]] to continue transferring data to the US on the basis of the FATCA agreement when that agreement is not in line with the GDPR.

Answer: no mention of the rights of data subjects

11[1]: Concept: Legally binding and enforceable instrument

Question: Does the instrument in question meet the criteria for being legally binding under relevant laws?

Context:Under national US law, Google LLC, as a provider of electronic communication services is subject to surveillance by the intelligence agencies and is thus obliged to provide the US government with personal data. According to the Schrems judgment, that the DPA considered up-to-date, this legislation doesn’t meet the requirements of EU law. Fourthly, considering that the SCC’s were not sufficient, the DPA assessed whether the controller and the processor implemented additional safeguards for the data transfers.

Answer: doesn’t meet the requirements of EU law

11[2]: same as 11[1]

11[3]: same as 11[1]

16[0]: Concept: Binding corporate rules

Question: Does the organization have binding corporate rules in place for data protection?

Context:The parties still agreed supplementary measures. First, Google has established policies and procedures and a team of qualified lawyers for handling authority requests for user data. Second, Google offers and the controller implemented the Anonymize IP feature and, finally, the controller had applied a redaction script on the website to prevent personal data unintentionally being shared with Google.

Answer: First, Google has established policies and procedures and a team of qualified lawyers for handling authority requests

17[0]: Concept: Binding corporate rules

Question: Have these rules been approved by the competent supervisory authority?

Context:First, the Irish DPA ascertained whether US law guaranteed an essentially equivalent level of protection of data protection rights in light of Schrems II. This was excluded by the supervisory authority, especially due to the lack of effective judicial remedies against the violation of data subjects’ fundamental rights by U.S. intelligence agencies and due to the lack of limitations imposed on the latters’ investigation powers. The latest developments in U.S. law (which are supposed to ensure a higher level of protection for data transferred to the U.S.) were deemed insufficient by the Irish DPA, especially since some of the promised reforms have not yet been implemented.

Answer: This was excluded by the supervisory authority

41[0]: Concept: Contractual clauses

Question: Does the organization incorporate specific data protection clauses in its contracts with third parties?

Context:Its servers were located in the EU. Company C included clauses in its offer stating that it would not disclose customer data to any third party, except as necessary to maintain or provide the services, or as necessary to comply with the law or a valid and binding order of a governmental body. After reviewing the offers, the publicly owned company issued a decision where it awarded the contract to Company A, as their evaluation of the price was the most economical.

Answer: Company C included clauses in its offer stating that it would not disclose customer data to any **Problem: not really a legal answer of whether that was enough**

42[0]: Concept: Contractual clauses

Question: Are these contractual clauses in compliance with the requirements of relevant data protection laws?

Context:Examining the decision in light of the provisions of the Charter, the Court held that the requirements of US national security, public interest, and law enforcement do in fact interfere with the fundamental rights of persons whose data is transferred there. These limitations on the protection of personal data were not circumscribed in a way that satisfied requirements that are essentially equivalent to those required under EU law. The principle of proportionality was also not satisfied, in so far as US surveillance programs are not limited to what is ‘strictly necessary’.

Answer: not **Problem: not talking about contractual clauses, at least not in the context above**

42[2]: Concept: Contractual clauses

Question: Are these contractual clauses in compliance with the requirements of relevant data protection laws?

Context:For the use of this tool, the controller transferred users’ personal data to the processor, in the US. The controller and Google had implemented standard contractual clauses (‘SCCs’) within the meaning of [[Article 46 GDPR]]. In 2020, ''noyb'' lodged a complaint with the Austrian DPA alleging that the controller breached the provisions of Chapter V GDPR.

Answer: yes **Problem: discussed before under SCC**

47[0]: Concept: Administrative arrangements

Question: Are these administrative arrangements consistent with data protection standards?

Context:Examining the decision in light of the provisions of the Charter, the Court held that the requirements of US national security, public interest, and law enforcement do in fact interfere with the fundamental rights of persons whose data is transferred there. These limitations on the protection of personal data were not circumscribed in a way that satisfied requirements that are essentially equivalent to those required under EU law. The principle of proportionality was also not satisfied, in so far as US surveillance programs are not limited to what is ‘strictly necessary’.

Answer: not **Problem: it does not mention which arrangement was chosen**

50[0]: Concept: Administrative arrangements

Question: Do these administrative arrangements provide clear channels for data subjects to enforce their rights?

Context:The DPA remarks that, according the Schrems II Judgment, the transfer of data to the United States may result in violations of fundamental rights, given that the US legislation allows for access to the data because of national security and public interest reasons. Such inferences are not reasonable, as limitations to fundamental rights are not clearly defined; as there are no clear and precise rules on the application of such measures or minimum requirements to protect against risks of abuse; there is no requirement for a necessity test; and there are no enforceable rights for data subjects or legal remedies. The Portuguese DPA found that the National Institute had not undertaken a sufficient Data Protection Impact Assessment, had not consulted the supervisory authority prior to processing, and had therefore not adopted adequate additional safeguards before using the services of a data processor who was headquartered in the United States.

Answer: no **Problem: it does not mention which arrangement was chosen**

50[1]: Concept: Administrative arrangements

Question: Do these administrative arrangements provide clear channels for data subjects to enforce their rights?

Context:These law allow for bulk collection of personal data. They do not allow a data subject to enforce any rights before a tribunal. ''With regard to national law relating to collection and processing of data:'' The French Court outlined that Article L. 1462-1 of the public health code provides for the Health Data Hub and the collection of health data from the existing national health data system (as per Article L. 1461-1).

Answer: They do not allow a data subject to enforce any rights before a tribunal **Problem: it does not mention which arrangement was chosen**

50[2]: Concept: Administrative arrangements

Question: Do these administrative arrangements provide clear channels for data subjects to enforce their rights?

Context:The principle of proportionality was also not satisfied, in so far as US surveillance programs are not limited to what is ‘strictly necessary’. It was noted that the provisions in the US surveillance programs neither limited the power they conferred onto national authorities, nor granted data subjects actionable rights before the courts against the US authorities. The Court proceeded to scrutinize the Ombudsperson mechanism that had been in place under the Privacy Shield, stating that it too did not provide data subjects with a cause of action before a body which was fully independent, and that this body was limited in so far as it could not impose rules that were binding on US intelligence services.

Answer: it too did not provide data subjects with a cause of action before a body which was **Problem: it does not mention which arrangement was chosen**

53[0]: Concept: Consistency mechanism

Question: Are there checks in place to ensure consistent application of data protection measures across the organization?

Context:The DPA concluded that Portuguese citizens lack any guarantees in regards to their data being collected by the National Statistical Institute, as US legislation does not offer a similar level of protection than the GDPR. The controller had neither been able to demonstrate that the data is not effectively transferred to the US, not had they implemented any supplementary adequate measures to ensure a similar level of protection, which they are obliged to do as a data controller. Therefore, the CNPD ordered the National Statistical Institute to suspend any processing of personal data for the census in the US or any other third country without adequate levels of protection, within 12 hours of their decision being issued.

Answer: not had they implemented any supplementary adequate measures to ensure a similar level of protection, which **Problem: questions refers to specific organization but the answer talks about different countries. Might be correct but still not enough information in the answer**

Questions-55-answers

* All answers with more than .65 confidence looks a part of an accurate answer/example with some exceptions
* The good ones are: 0, 1, 5, 10, 17, 21,

Exceptions:

* 11:1
* 53:0
* 42:0
* 47:0

Some examples of accurate with smaller values

* 0.58 - 16:0
* 0.55 - 25:0
* 0.42 - 39:0
* 0.48 - 41:0

Comments:

* The exceptions above show that legal terms in the questions should be weighted more than other terms.
* The sentences which are returned talk about the topic in the question but normally do not provide the answer. We should use it as a first step to find relevant sections and court decisions but then we need to extract the relevant answer which is around the matched sentence (probably directly before or after).