Prompt

You are a data protection officer for the company, "Infotech", which provides IT services and is headquartered in Dublin, which is subject to Irish and EU legislation. You have been asked by management to write a report on the legal requirements related to data protection in Ireland and the EU, which should cover:

- An overview of the legal requirements related to privacy and data protection that the company should consider in it's data governance and how it might address those requirements in practice, identifying the most significant legal provisions it would need to address.
- The company is considering the need to engage a data processor. Discuss the relationship and the roles and responsibilities of a data controller and a data processor relevant in this event.
- The company needs to transfer data to the US and UK. Describe what aspects the company needs to consider for the data transferring agreement and what the implications would be for the company.
- How Infotech can ensure that it's third-party service providers comply with GDPR and other data protection regulations when processing personal data on behalf of Infotech

Response

As an Irish ITS company, Infotech are subject to Irish and European Union legislation regarding data protection, data privacy and data rights. These rights are enshrined in law and there are multiple laws that deal with this.

The right to privacy is a long running concept. It was first enshrined in Article 12 of the UN's Universal Declaration of Human Rights (1948) [1], and then further enshrined in Article 8 of the European Convention on Human Rights (1950) [2], signed into Irish law in 2003 [3]. There is also the EU Charter of Fundamental Rights, declared in 2000 [4] and signed into Irish law in 2009 along with the Lisbon Treaty [5], that standardises the rights for each citizen in the EU. It's worth noting that the right to privacy, and by extension, data privacy, is only present in charters. Bunreacht na Eireann does not have any provision regarding the right to privacy.

Regarding the right to privacy, the right to a private life, to be autonomous, in control of information about yourself, to be let alone, plays a pivotal role [6]. They also have a right to limit the sharing of their personal information to any other person or organisation, with some exceptions [7], such as some legal cases. With respect to said person's privacy, any person who is accessing and processing this information must have regard to these principles: 1) the information is confidential, 2) the information is communicated in the confidence of confidentiality, and 3) there must be no unauthorised use of the information.

There is also the notion of personal data, which is any identifiable data. Under this, there are special categories of personal data, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biometric data, and data concerning a person's sex life and sexual orientation. Also, Genetic, biometric and health data are of particular importance.

There is also the notion of processing and a data processor. A data processor is someone who processes data on behalf of a data controller, who is the person who controls the data. Therefore, if Infotech were to process any data, Infotech would be a data processor. Examples of data processing include: collection, organisation, storage, alteration, recording, structuring, etc. There is also the data subject, of whom the data is about [8].

The right to privacy has been enshrined in the prior EU Charters, which are both enshrined in Irish law. However, in the era of computing and the information age, data has become a serious threat to the right to privacy and should be considered within that. Thusly, there have been multiple directives and acts passed to regulate the processing of data.

However, the primary law governing this on a European level is the General Data Protection Regulation (2018) [9]. This law is in effect on all members states of the EU. The law aims to standardise data privacy laws across Europe and applies to all organisations that handle personal data of EU residents. Importantly, this is not limited to the EU. So, the processing of any European person must be subject to GDPR, regardless of whether the processing is done outside of the EU. So, a company could not try to circumvent GDPR by engaging a data processor who is based outside of the EU, as these processors would still be subject to the same legislation as the EU company.

Under GDPR, data processed may only take place after explicit consent from the data subject – consent that is freely given, specific, informed, and unambiguous. This must be an active exercise – silence, inactivity or a pre ticked box do not constitute consent. Furthermore, the data subject must have the right to easily withdraw their consent at any time and must be informed prior of their right to withdraw consent. However, any data processed

before consent is withdrawn is legal. In addition, the controller must be able to prove consent is given, and consent cannot legally infringe on GDPR. So, a person cannot consent to waive protections that are in place via GDPR. Also, the processing of a child's data requires consent from the child's guardian [10].

GDPR is primarily concerned with personal data, so any personal data falls under the scope. It should be noted that data that is pseudonymised falls under the scope, while anonymous data does not. GDPR is based on 7 data protection principles: use must be fair, lawful and transparent, there must be a limit on the purpose of processing, the data processed must be minimised, data must be accurate, the data storage must be limited, the processor/controller must act with integrity and confidentiality, and the processor/controller must be accountable to any failings [11].

The law also imposes strong rights to individuals and responsibilities to data processors and controllers. It empowers regulators to impose heavy fines of up to €20 million, or 4% of the global turnover, whichever is higher, at the higher level, and up to €10 million, or 2% of the global turnover at the lower level [12]. These fines have been imposed quite heavily. Meta, due to Instagram's failings, was subject to a fine of €405 million in 2022 [13], and then another fine of €265 million, again in 2022 [14], after failings by Facebook. Similarly, Amazon was subject to a fine of €746 million in 20211 [15].

These fines were imposed by the Data Protection Commission [16], who are the Irish data regulatory body, who enforce GDPR, and who were established following the Data Protection Act of 2018 [17]. This act gives further strength to GDPR (particularly around areas of digital consent), and some exceptions to GDPR under Irish law. It also defines the notion of children. This follows from the GDPR principle of subsidiarity, which allows for member states to have some standing on how certain issues are regarded.

A notable example of this is that, under Irish law, GDPR's laws around processing and retention of personal data does not apply under circumstances where that data is subject to law enforcement purposes [18]. Instead, the Law Enforcement Directive applies. [19] This became a notorious issue during the trial of Graham Dwyer, where the state used data collected from his phone [20], This argument was also used in other trials until the Court of Appeals overruled Dwyer's appeal [21].

There are some other notable exceptions to GDPR. Firstly, deceased people are not subject to GDPR. Additionally, legal persons do not have protection from GDPR, only natural persons. Thusly, any legal persons have few protections from GDPR. Furthermore, there are some instances, depending on the circumstances, time and type of data being processed, that the GDPR will not apply, and another legal framework will take effect. For example, if an infringement came before 25th of May, then GDPR cannot take effect.

To summarise, the primary thing that needs to be considered is GDPR and the DPA, and the obligations that places on a data controller. The privacy of any personal data must be protected and must be kept confidential, or risk steep fines stemming from failures to uphold these principles.

There may be a scenario however where Infotech would prefer to outsource the data processing. This would require engaging a data processor. This can be a very helpful tool, however, it's important to remember that this also comes with a large number of additional issues that must be addressed.

As mentioned previously, a data controller is someone who controls the data and decides what will be done with it. In this scenario, Infotech would be the data controller. A data controller determines the how and why of the data being processed. Consequently, the data controller is subject to responsibilities they owe to the data subject. The data subject is the person about whom the data refers.

A data processor then is someone who processes the data on behalf of a data controller. Sometimes, the data controller can process it themselves, in which case they are both, and sometimes, it is done separately. Data processing includes: collection, organisation, storage, alteration, recording, structuring, etc.

It's important to remember that ultimate responsibility to the data subject lies with the data controller. So, if Infotech were to engage a data processor, it must be paramount that Infotech recognises their responsibilities to the data subject. These are the responsibilities that were set out previous regarding GDPR. So, Infotech must protect the data, treat the data confidentially, maintain a data subject's right to privacy, etc [22].

So, Infotech, given its role as a data controller, will be ultimately responsible for any processing that is engaged in, regardless of whether Infotech is the one doing it. Hence, Infotech will be subject to GDPR and the DPA in any event. Thus, when selecting a processor, the controller has some obligations that must be followed. For

example, a controller must ensure that a contract or another legally binding agreement has been signed. This contract must have some specific sections to protect the data subject.

The processor must be accountable to the data controller and maintain in's compliance with the regulatory requirements. Given that Infotech are an Irish based company, this means that the controller must be compliant with GDPR in the same way that Infotech is. The processor must also offer a minimal of security that is defined by the controller, to ensure the data is protected from breaches, etc. The processor must also only undertake to processing specific data after specific instructions by the data controller. This means that the processor can only process exactly what it's been asked to process by the controller and no more. The processor must then make sure that any individuals who are doing the processing are subject to the confidentiality requirements necessary. Furthermore, the processor cannot appoint an additional data processor without the express consent of the controller. Finally, the processor must maintain written records of all actions undertaken.

Regarding the controller, their obligations are as follows:

The controller must ensure that a contract with the above specifications has been signed by the data processor prior to any engagement in processing. The controller must also give specific instructions regarding the data to be processed. Furthermore, the controller must have a section in the contract regarding what happens to the data afterwards. Finally, the controller must be informed of the reputation of the processor, as it's their responsibility to ensure the data is processed correctly.

These obligations must be met for a data controller to engage a data processor for data processing purposes. In essence, the data controller is subject to the responsibilities it owes to the data subject at every point, and it is the responsibility of the controller to engage in a processor that can be trusted and that can ensure that the data remains secure.

In selecting a data processor, it's important to remember that there is a special category of transfers that may arise when picking the processor. If the processor operates outside of the EU, then InfoTech must have regard to the legislation regarding International transfers outside of the EU. Within the EU, it's all within the remit of GDPR. However, when transferring data to outside the EU, the GDPR has a specific provision – Chapter V (Articles 44 to 49). This system allows for a tiered approach. However, under the general principles (article 44), the provisions in the chapter will maintain the protection guaranteed by the GDPR [23].

There are three main transfers that are acceptable: transfers on the grounds of an adequacy decision, transfers subject to appropriate safeguards, and derogations for specific situations.

A transfer on the basis of an adequacy decision (article 45, Chapter V, GDPR) is the ideal form of transfer. This is a transfer to a third country whereby the commission considers that the country in question offers an adequate level of protection to the EU member, based on an assessment on grounds including: rule of law, respect for human rights, relevant legislation, etc.

In 2021, the EU found that the UK's legislation and data protection was adequate, and as a result, a transfer on the basis of an adequacy decision can be made between the EU and the UK [24]. However, the EU found that America did not offer an adequate level of protection, and so, a different approach must be taken.

Formerly, there was an EU-US Safe Harbour agreement [25], which allowed for a transfer of data. There was then an EU-US Privacy Shield [26], which was a framework which allowed for certain transfers of data to certain companies who were self-certified, but this was found to be inadequate. The issue arises due to mass surveillance operations in the USA, and the lack of privacy that GDPR protects against [27]. Thus, any transfer must be subject to appropriate safeguards. Thus, this transfer would fall under Article 46 of GDPR. However, it's important to note that currently there is a lot of legal uncertainty around transfers between the EU and the US [28].

There are also some exceptions, such as the "Umbrella Agreement", which allows for transfers between the US and EU on the basis of law enforcement purposes. This would fall into Article 49 of GDPR – derogations for specific purposes. This agreement has been certified by both the US and the EU [29].

Currently, there is a framework being drafted called the EU US Data Privacy Framework which will allow for more flowing of data between the US and the EU, potentially leading to an adequacy decision [30]. However, this has not yet come into effect and there are outstanding issues that must be addressed, and, as of one month ago, the European Parliament rejected the bill as in its current form, citing the need for a lawsuit proof regime to ensure legal certainty [31].

Thus, given that InfoTech is acting as a data controller, the responsibilities of all these data rights guaranteed by the EU and GDPR that have been outlined in this report are the responsibility of InfoTech. Therefore, any third-party service provider must be compliant with GDPR, and InfoTech must ensure that this remains the case [32]. There are a range of ways that InfoTech can ensure compliance.

As mentioned, the primary method is via a contract. Any third-party service provider that processes data on behalf of InfoTech is obligated to sign a contract before engaging into any processing. This contract must stipulate a multitude of things including: the exact nature of the processing, what happens to the data after the project is finished, etc. This contract is an immediate legal protection for InfoTech [33].

However, it's also important to use a verifiable third party. A third party should be chosen with some wariness regarding their reputation. Furthermore, the third party should be in a place where the protections are easily applied. For example, it would be much easier to deal with a third party in Europe rather than a third party in the US, due to the issues with data transfers mentioned previously. It would also help if the service provider were in a country where GDPR is in effect regardless.

Ultimately, there should be both a legal and a common-sense approach to ensuring the protections remain and that the third-party service provider remain complaint with GDPR. At the end of the day, the responsibility lies with InfoTech.

References:

[1] https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2012,against%20such%20interference%20or%20attacks.
[2] https://www.echr.coe.int/documents/convention_eng.pdf
[3] https://www.ihrec.ie/download/pdf/ihrec_human_rights_explained.pdf
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
[5] https://www.europarl.europa.eu/factsheets/en/sheet/5/the-treaty-of-lisbon
[6] https://edps.europa.eu/data-protection/data-protection_en#:~:text=Privacy%20%E2%80%93%20a%20fundamental%20right&text=The%20right%20to%20privacy%20or,Fundamental%20Rights%20(Article%207).
[7] https://iapp.org/resources/article/privacy-act-exceptions-2/
[8] https://www.dataprotection.ie/en/individuals/data-protection-basics/definition-key-terms#:~:text=The%20term%20'personal%20data'%20means,a%20'data%20subject').
[9] https://gdpr-info.eu/
[10] https://gdpr-info.eu/issues/consent/
[11] https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection
[12] https://gdpr-info.eu/issues/fines-penalties/#:~:text=83(4)%20GDPR%20sets%20forth,to%20that%20used%20in%20Art.
[13] https://www.theguardian.com/technology/2022/sep/05/instagram-owner-meta-fined-405m-over-handling-of-teens-data
[14] https://www.euronews.com/next/2022/11/28/meta-hit-with-265-million-fine-by-irish-regulators-for-breaking-europes-data-protection-la
[15] https://www.irishtimes.com/business/technology/amazon-hit-with-746m-eu-fine-for-data-privacy-rule-breaches-1.4634930
[16] https://www.dataprotection.ie/en/who-we-are
[17] https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html
[18] https://www.dataprotection.ie/sites/default/files/uploads/2019-05/190507%20Data%20Protection%20Basics.pdf
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG
[20] https://www.irishtimes.com/news/crime-and-law/courts/criminal-court/dwyer-appeal-likely-to-focus-on-phone-data-and-questioning-1.2159181
[21] https://www.irishtimes.com/crime-law/courts/2023/03/24/graham-dwyer-fails-in-appeal-against-conviction-for-murder-of-elaine-ohara/
[22] https://www.dataprotection.ie/en/organisations/know-your-obligations/controller-and-processor-relationships#:~:text=Processors%2C%20for%20example%2C%20must%20only,the%20processing%20of%20personal%20data.
[23] https://www.dataprotection.ie/en/organisations/international-transfers/transfers-personal-data-third-countries-or-international-organisations
[24] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183
[25] https://www.experian.co.uk/business/glossary/safe-harbour-agreement/
[26] https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216
[27] https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded
[28] https://www.matheson.com/insights/detail/legal-certainty-ahead-for-eu-us-data-transfers
[29] https://ec.europa.eu/commission/presscorner/detail/it/MEMO_15_5612
[30] https://ec.europa.eu/commission/presscorner/detail/it/MEMO_15_5612
[31] https://iapp.org/news/a/european-parliament-committee-rejects-eu-us-dpf-us-international-trade-admininistration-seeks-stakeholder-feedback-on-transborder-frameworks/
[32] https://www.dataprotection.ie/en/organisations/know-your-obligations/data-security-guidance
[33] https://www.dataprotection.ie/en/organisations/know-your-obligations/controller-and-processor-relationships