November 2019

www.chalmindataprivacy.ie

Welcome to this month's newsletter. In our feature piece we have chosen to highlight Breach Procedures.

As part of your company's data protection policies, you should put together a procedure that will allow you to respond quickly and efficiently when your customers' data security has been compromised.

Responding quickly is extremely important because it means that you can limit the damage done – both to the individuals affected and to your company. The good thing is that a Data Breach Notice Letter is a document that you can prepare partly in advance as part of your data breach policy.

If you suffer a serious data breach, you're required to inform your Data Protection Authority and in many cases, the individuals whose data may have been compromised. A Data Breach Notice Letter is a way for you to do this. The GDPR is not there to put the brakes on your business. When implemented properly, it is there to increase trust between you, your employees, suppliers and customers alike.

We can help you put a robust and manageable procedure in place, for more information contact us gail@chalmindataprivacy.ie

Brexit: Advice from our August newsletter that is worth repeating.

Are you an Irish company that transfers personal data to the UK ?

The proposed withdrawal agreement would have preserved the status quo in data protection terms, at least until the end of the transition period in December 2020. However, if the U.K. leaves the EU without a deal, the implications for international data flows and privacy compliance generally will be severe. Without additional actions, UK-based processing of EU personal data will be illegal.

There are numerous ways you might be transferring data to a UK-based company, such as the following examples;

- Are you outsourcing your HR, IT or Payroll function to a UK based organisation?
- Are you using a UK based marketing company to send marketing communications to your customer database?
- Is your pension scheme based in the UK?
- Are you using a UK based company to analyse data on visitors to your website?
- Are you storing data in the UK on a server or in the cloud?

In a 'No Deal' Brexit scenario you will need to put extra measures in place to legally transfer this data. EU based data controllers are not permitted to transfer personal data outside the EU/EEA unless those standards are maintained.

In a “no-deal” Brexit scenario, the UK will no longer be a member of the EU; instead, it will become a ‘Third Country’. It will have to look for an Adequacy Ruling like Japan in time. This means that transfer of personal data from Ireland to the UK will be treated in the same way as transfers of personal data to countries like Australia or India etc.

What this means in practice is that, in order to comply with GDPR rules, an Irish company intending to transfer personal data to the UK will need to put in place specific safeguards to protect the data in the context of its transfer and subsequent processing. This can be done in a number of different ways, depending on the circumstances in which the data is to be transferred. One such way is the use of “Standard Contractual Clauses” or “SCCs” or” Model Clause Agreements “and this is likely to be relevant to most Irish businesses that transfer personal data to the UK.

The Model Clause Agreements consist of standard or template sets of contractual terms and conditions that the Irish-based controller and the UK-based recipient both sign up to. The basic idea is that each of the parties to the contract gives contractually binding commitments to protect personal data in the context of its transfer from the EU/EEA to the Third Country. Importantly, the data subject is also given certain specific rights under the SCCs even though he or she is not party to the relevant contract.

Fines across Europe

In relation to Third party processor contracting under the GDPR the President of the **Polish Personal Data Protection Office** has imposed an administrative fine of EUR9,400 (PLN40,000) on a public entity for failure to comply with, inter alia, Article 28(3), GDPR. The mayor of the city failed to conclude a personal data processing agreement with third parties who personal data was shared with. Therefore, there was no lawful basis upon which the data was processed.

This should serve as an Important wake up call in relation to Third party processor contracting under the GDPR.

https://edpb.europa.eu/news/national-news/2019/polish-supervisory-authority-imposed-first-administrative-fine-public-entity_en

The Berlin Data Protection Commissioner imposed a fine on real estate company.

On 30 October 2019, the Berlin Commissioner for Data Protection and Freedom of Information issued a fine of around € 14.5 million against Deutsche Wohnen SE for violating the General Data Protection Regulation (DS-GVO).

The company has used an archive system for the storage of personal data of tenants.According to the authority, no health data is affected & no data has been passed on to third parties. According to the authority, Deutsche Wohnen wanted to be on the safe side when it came to storing tenant data & comply with legal requirements - housing companies have certain obligations to maintain data. However, the retention obligations do not apply according to the opinion of the DPA to the objected categories of personal data. "There are different deletion periods depending on the category".In response to the question as to what Deutsche Wohnen should have done differently, the state commissioner answers that there are technical systems that can help to separate data with different deletion requirements. "The company even had such a system. But they did not use it accordingly".

The fourth highest GDPR fine has been issued **towards Swiss Post**. Once again, we gain clarity in how and when the legal grounds can be used, and the need to be precautious when handling sensitive personal data. https://aigine.se/en/selling-a-register-price-e18-000-000/gdpr/

The Polish DPA fined a company 201.000 PLN (47000 EUR) for making withdrawal of consent not 'as easy as it was to give'. Data subjects were required to state the reason for unsubscribing from direct marketing e-mail and the messages were misleading.

The Romanian DPA announced it has imposed a GDPR fine of EUR 11,000 on a courier services company for breach of Article 32 paragraphs (1) and (2).

According to the DPA, the fine was issued for failure of the controller to implement appropriate technical and organisational measures which led to the loss of and unauthorized access to personal data (name, bank card number, CVV code, card holder address, personal identification number, ID card series and number, bank account number, approved credit limit) of approximately 1,100 data subjects.

Closer to home

The Data Protection Commission Ireland has updated its guidance on subject access rights and removed confusing references to "third-party personal data" which was leading some controllers to unlawfully redact all references to other people from SAR responses

New Guidance

EDPB guidelines on Controller relationships is here

https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf

Damages

For the first time in the EU, a court has awarded a data subject compensation **for emotional harm**, after the unlawful processing of their data.The Austrian postal service, was found to have stored political data of approximately two million customers, using profiling to predict their political orientation. None of these customers were aware of this and they did not consent to it. A claimant has argued that he was so disturbed by this that he suffered emotional harm which warranted compensation. The Regional Court of Feldkirch at first instance held that the mere feeling of being disturbed constitutes immaterial harm and awarded the claimant €800 of the €2,500 claimed.The Court has pointed out that not every inconvenience will give rise to a claim for damages-

Tip of the month

Your Privacy Notice needs to be correct. Privacy has officially become something a brand can market. It also has the effect of raising awareness on the issue generally. I saw an Interesting post on LinkedIn for all those fence-sitters waiting for enforcement**.**

“Congrats to the potential supplier we've just ruled out, based entirely on their awful website.1 - No privacy policy.2 - No cookie consent option (despite dropping 16 cookies).3 - No company info so I have no idea who they really are.4 - Asks for my contact details before showing me anything about the company or its products(4a - Doesn't tell me what happens to the data if I do give it to them)They lost us as a customer before they even knew we existed because if they can't get the website right, it's unlikely they can get the rest right”