NEWSLETTER MAY 2019

International News

Denmark: Call Recording Fine

Denmark supervisory authority decided that affirmative consent is required when companies record customer telephone calls. This means that companies need to inform people about the fact that the call is recorded and allow them to opt-out (meaning stopping the recording).

The supervisory authority rejected the telecom company's arguments that its recording practices served a legitimate interest (improvement of customer service).

Chalmin Data Privacy recommendations:

➡ Make sure your script informs the customer about the processing.

➡ Make sure that you seek active consent for the recording.

➡ Make sure that you have a "stop recording" switch that can be flicked by the operator.

➡ Make sure that the consent can be withdrawn by the customer.

➡ Make sure you inform the customer and seek active consent in just a few seconds without upsetting the customer

https://www.natlawreview.com/article/denmark-dpa-rules-how-gdpr-applies-to-voice-recordings?amp

Italy: First GDPR Fine and Article 32 Security Measures

The Italian Data Protection Authority has imposed its first gdpr fine for €50k for failure to implement adequate security measures to protection personal data.

The DPA imposed the fine on a data processor for failing to take proper security measures following a 2017 data breach. This is interesting as the DPA did not give the data controller any consideration in respect of the breach; rather, it went directly after the processor.

Failures:

(1) vulnerability assessment performed was no longer updated by the processor, making the implementation of patches extremely complicated and time consuming;

(2) not implementing a system aimed at strengthening passwords to be used for the creation of the accounts and to avoid the risk of brute force attacks;

(3) not securing protocols and digital certificates to protect data during their transit and reduce the risk for users to be attracted by fake sites;

(4) inadequate solutions aimed at increasing the level of security of the storage of passwords due to the weak cryptographic algorithms;

(5) security measures aimed at anonymising personal data were considered to be not adequate; and

(5) shared accounts used by system administrators had unduly large privileges granted.

https://www.gamingtechlaw.com/2019/04/first-gdpr-fine-italy.html

Germany: Facebook targeted audience breach

Online shops and marketers routinely share customer data with Facebook to reach them with targeted advertising. Turns out: in many cases this is illegal. A ground-breaking decision by a German Data Protection Authority recently ruled that matching customers' email addresses with their Facebook accounts requires their explicit consent.

https://netzpolitik.org/2019/facebook-custom-audience-illegal-without-explicit-user-consent-bavarian-dpa-rules/

Technical thoughts

Password guidance.

We are not IT specialists but from our experience the following is a guide aimed to advise data controllers (e.g., service providers, administrators) on how to set up effective password policies and securely store passwords, and data subjects (users) on how to choose secure passwords.

A password-username authentication is a technical and organizational measure pursuant to Art. 32 of the GDPR, which requires that data controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk that the processing would otherwise present to individuals. Such measures must include the ability to ensure the ongoing confidentiality and integrity of processing systems and services. EU regulators have already decided that passwords should never be stored unencrypted. Data controllers should also consider implementing a two-factor authentication and to protocol failed attempts to log into a user's account. The guideline also recommends that data controllers and processors give guidance to their users on how to set up secure passwords and, as a best practice, implement minimum requirements for users to set and to periodically update their passwords. For failing to comply with these requirements, data controllers and processors can be subject to fines.

For the user, it is recommended that he or she use different passwords for each account. The differences between each password should be substantial, and a secure password should contain at least 12 characters, including capital letters, digits and punctuation. In addition recognisable words should not be used as part of the password as this can be used in dictionary/brute force attacks. Similarly our guidance will be that standard endings/starts should not be used – e.g only the first letter is CAPS, ends in an ! , or _1 etc

Thought Leadership articles

Navigating GDPR: 5 Common mistakes in a Privacy policy

Chalmin Data Privacy is often called in to help businesses review or establish good GDPR practice, we help businesses of all sizes navigate this complex area and despite the GDPR having been in place now for over 10 months, from small start-ups to prospering SME's there are still plenty of businesses that are struggling to comply.

So as we approach the anniversary of its introduction, I thought I would share some of the common mistakes we see around a privacy policy. Whilst I could easily have made the list significantly longer, I wanted to make sure the article didn't run to multiple pages, and also make it a manageable start-point for businesses looking to comply with this important legislation.

1. **The policy scope**. A simple one to start with, and also most common - the policy should not only refer to the data processed on the website site but to all the services provided to the customers and the processing required for them.
2. **Disclosure of personal data**. Everyone swears they do not share the data with unauthorized entities and obviously they do not sell them. What they "forget" to mention is exactly what data is disclosed and to whom. The biggest problem is that often they do not even know or realise themselves that using third-party platforms, tools or services means disclosing personal data (for example Internet providers, hosting services, social media platforms, payment services online, as well as all entities that have third party cookies on their site, as well as their partners). The rule here is simple – check every touchpoint for the data to build a full picture and if you don't have that expertise or resource in house, bring in a consultant that does.
3. **Data transfers outside the EU / EEA** and protection measures - must be specified.. Most times, in the case of companies belonging to a group, they do not even mention the countries where the transfer is made within the groups ... for example, if the IT services at group level are in India or Turkey ie outside of the EEA., this is often not mentioned, although there is a transfer of almost all personal data within the group through its It services. One solution is applying BCRs(binding corporate rules) , which form a legally binding internal code of conduct operating within a multinational group, which applies to transfers of personal data from the group's EEA entities to the group's non-EEA entities. . BCRs are legally binding data protection rules with enforceable data subject rights contained in them, which are approved by the competent Data Protection Authority. Another solution is intra group model clause agreements.
4. **Consent** – This is often where companies I help think they have a bullet-proof solution but have actually failed to think about the entire set of requirements that GDPR demands. It Is not enough to say "We have requested the customer's agreement and have proof that he/she has agreed." For consent to be valid it must be explicit, informed and freely given. Is consent buried in a large document referring generally to a multiplicity of types of processing valid.? It is a requirement to be transparent (i.e. to clearly and precisely tell the individual how his data is going to be processed) to do otherwise is a violation of the GDPR principles.
5. **Security** or **integrity and confidentiality of personal data** – taking "appropriate" technical or organisational measures. Those appropriate measures should at the very least make sure that the website has an SSL certificate, as the organisations

invariably send sensitive personal information on insecure channels otherwise. Another appropriate measure that is often under deployed, is encryption.

Whilst this is not an exhaustive list, it is a useful prompt to review some of the biggest pitfalls that we at Chalmin Data Privacy regularly come across; And whilst Brexit still lacks clarity, what we can be sure of, from recent high profile cases across the EU, is that the compliance requirements for GDPR are crystal clear.

For more information visit http://www.chalmindataprivacy.ie