October 2019

www.chalmindataprivacy.ie

Welcome to this month's newsletter. In our feature piece we have chosen to highlight the Planet 49 Case and Cookies et al:

Cookies et al.

On 1st of October 2019, the European Court of Justice gave an important decision regarding the e-Privacy directive in a case C-673/17 (Planet 49 case).

There are a number of important lessons to be learned from that ruling. Firstly, a consent from the end users must be obtained before placing cookies on the end users' end terminal. Secondly, such consent must meet the requirements of the GDPR.

It is also worth noting that the applicability of Article 5(3) of the e-Privacy directive is wider than just cookies. In fact, it applies to 'storing of information or the gaining of access to information already stored, in the terminal equipment of an end user' if this is not 'strictly necessary' in order for the 'provider of an information society Service' explicitly requested by the end user. This has wide reaching implications for the ad tech industry

Some major point arising out of this case:

(1) pre-checked boxes do not satisfy consent requirements under 95 directive, e-Privacy, and GDPR;

(2) consent requirements do not change if the data held/accessed by the cookie is not personal data;

and

(3) users must be informed of the duration of the cookie and whether third parties will have access to the data.

Nearly 90% of Websites therefore are not compliant.

http://curia.europa.eu/juris/document/document.jsf;jsessionid=2E1AEC84F6BD0CF3D466B41DBF1AF383?text=&docid=218462&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1447544

Online services

The EDPB(The Overseeing Board) has issued final guidelines on the "necessary for the performance of a contract" legal basis under the GDPR. These Guidelines 2/2019 are on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.

By way of background Article 6(1)(b) GDPR provides a lawful basis for the processing of personal data to the extent that "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract". This supports the freedom to conduct a business and that there are contractual obligations towards the data subject cannot be performed without the data subject providing certain personal data. If the specific processing is part and parcel of delivery of the requested service, it is in the interests of both parties to process that data, as otherwise the service could not be provided, and the contract could not be performed. However, the ability to rely on this or one of the other legal bases mentioned in Article 6(1) does not exempt the controller from compliance with the other requirements of the GDPR.

.

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en

- To benefit from this legal basis controllers must be able to show that both that (i) the processing takes place in the context of a valid contract with the data subject that and (ii) processing is objectively necessary in order that the particular contract with the data subject can be performed.

- Merely referencing or mentioning data processing in a contract is not enough.

- This legal basis may apply to certain actions that can be reasonably foreseen and necessary within a normal contractual relationship, such as sending formal reminders about outstanding payments or correcting errors or delays in the performance of the contract.

- Contractual warranty may be part of performing a contract, and thus storing certain data for a specified retention time after exchange of goods/services/payment has been finalized for the purpose of warranties may be necessary for the performance of a contract.

- Returning goods or payment after a contract is completed may fall under this legal basis.

- Processing for behavioural advertising is not necessary for a contract.

What does that mean?

Assessing what is 'necessary' involves a combined, fact-based assessment of the processing "for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal". If there are realistic, less intrusive alternatives, the processing is not 'necessary'. Article 6(1)(b) will not cover processing which is useful but not objectively necessary for performing the contractual service or for taking relevant pre-contractual steps at the request of the data subject, even if it is necessary for the controller's other business purpose.

Article 32 of the GDPR and Security

All Organisations big and small need to improve their security measures to be able to comply with the requirements of the GDPR and most especially article 32

1. "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
    a the pseudonymisation 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 organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

We would also recommend Encryption. Take for example transferring personal data by USB device.USB devices such as memory sticks or external hard drives offer a convenient way to transfer data. However, their small physical size and large data capacity means that large volumes of personal data can be lost or stolen with relative ease.

Personal data can be encrypted by placing the files within an encrypted container on a USB device, but this requires the recipient to have access to the same encryption algorithm or software.

Hardware-encrypted USB devices are also available which contain the necessary encryption capability embedded within the device, meaning that the data can be decrypted without the need for the user to install additional software. However, due to the security risks present in permitting the use of USB devices, it is possible that you have implemented policies which forbid or technically limit the functionality of USB devices within your network. In this case you would need to consider how you might transfer data to these devices, and likewise how you would access data on any you receive.

You also need to consider a method to transfer the key or password to the recipient over a separate communication channel.

The Hungarian National Authority for Data Protection and the Freedom of Information recently fined a Controller 15,150 for insufficient fulfilment of data breach obligations. The data controller did not fulfil its data breach obligations when a flash memory with personal data was lost.

Fines across Europe

Turkish authorities have fined Facebook Inc (1.6 million lira ($282,000) for violation of data protection laws which affected 280,959 Turkish users who had their personal information, including names, dates of birth, location, search history and more, impacted by the privacy breach.

https://mobile-reuters-com.cdn.ampproject.org/c/s/mobile.reuters.com/article/amp/idUSKBN1WI0LJ

Greek Fine shows the Importance of opt Out systems that actually work.

The Greek DPA fined the Hellenic Telecommunications Organization for;

1. Violating the principle of accuracy and data protection by design while keeping subscribers' personal data.

The DPA received complaints from subscribers who, despite having opted-out, had received telephone calls from third parties for the purpose of promotion of products and services. The DPA imposed an administrative fine of EUR 200,000.

2. Non-compliance with the right to object and infringement of the principle of data protection by design while keeping subscribers' personal data

The DPA received complaints from the Company's advertising message recipients about their inability to delete them from the list of acceptable advertising messages. An examination of the complaints revealed that, since 2013, due to a technical error, deleting through "unsubscribe" link did not work. DPA found an infringement of the Article 21(3) and Article 25 and imposed an administrative fine of EUR 200,000.

https://www.dpa.gr/portal/page?_pageid=33,15453&_dad=portal&_schema=PORTAL

GDPR fine in Romania: the Romanian Data Protection Authority fined the Romanian bank Raiffeisen Bank SA €150,000 for using WhatsApp to share individuals' data, recognizing that WhatsApp is not a sufficiently secure means of communication to share personal data.Raiffeisen Bank Romania carried out scoring assessments on the basis of personal data of individuals registered on the Vreau Credit platform provided by the platform's staff via WhatsApp and then returned the result to Vreau Credit using the same means of communication.

https://edpb.europa.eu/news/national-news/2019/company-fined-150000-euros-infringements-gdpr_fr

Closer to home in Ireland

The Data Protection Commissioner's office budget is up by 1.6m as announced by the Budget. The total Budget for 2020 is 16.9m**.**

Ireland's Data Protection Commissioner has concluded investigations into Facebook's WhatsApp and Twitter over possible breaches of EU data privacy rules we are told, and the investigations will now move into the decision-making phase.

Companies can be fined up to 4% of global annual revenues for breaching Europe's data privacy rules.

Tip of the month re Safe browsing

You need to install a secure certificate (often referred to as SSL but should be TLS 1.2 as a minimum since SSL is an older protocol that shouldn't be used anymore) to provide encryption between the browser and your web application. It's referred to as "https" and the website should show a small padlock .