NEWSLETTER September 2019

Feature article from Gail Chalmin

Welcome to this month's newsletter. In our feature piece I have chosen to highlight Biometric Data processing.

To be legally compliant with data protection law, an employer must have a "lawful basis" or justifiable reason to process an employee's personal data. As required under the current data protection regime, and in the GDPR, these reasons could include:

- Employee consent
- Where the processing is necessary for the performance of a contract to which the data subject has agreed to
- For compliance with an employer's legal obligation
- Where the processing is necessary for the purposes of legitimate interests pursued by the employer
- When it is n the public interest.

Biometric data used to uniquely identify individuals is considered a special category of personal data under the GDPR. Processing of special categories of personal data is prohibited unless an 'exception' applies.

Explicit consent given by the data subject to process their biometric data is one of these 'exceptions', however employee consent is often not considered true consent due the balance of power stacked in favour of the employer in the employer/employee relationship. Legitimate interests are not available as an exception to this prohibition.

However, considering the stricter consent obligations under the GDPR and the Article 29 Working Party guidance now the overseeing body the EDPB, an employer should seek alternative bases to explicit consent to process its employees' biometric data. Employers cannot rely upon legitimate interests to process biometric data of employees.

Accordingly, employers must rely upon another legal basis to use biometric data for secure access to their place of employment. Unless an employer can make a legitimate argument that it is processing biometric data for the vital interests of its employee, or is doing so in the public interest, no other alternative basis is currently available.

In my opinion, the employees should be offered an alternative to the biometric hand clock in system maybe a fob system could be utilised in tandem.

Kind regards
Gail Chalmin

First fines for Biometric data breaches are appearing

This is a link to the recent Swedish School fine for biometric data processing.

https://edpo.brussels/news/swedish-data-protection-authority-issues-first-fine-biometrics-use-under-gdpr

In addition and following the EDPB's Opinion the Irish Data Protection Commission (**DPC**) has published a non-exhaustive list of processing activities (**DPIA**) to be carried out. The list encompasses both national and cross-border data processing operations. It should be read in conjunction with Article 35 of the GDPR and the Article 29 Working Group Guidelines

When is a DPIA required?
The DPC has determined that a DPIA will be mandatory for the following types of processing operations:

1. Use of personal data on a large-scale for a purpose(s) other than that for which it was initially collected (a compatibility test must also be carried out pursuant to Article 6(4) GDPR).
2. Profiling vulnerable persons including children to target marketing or online services at such persons.
3. Use of profiling or algorithmic means or special category data as an element to determine access to services or that results in legal or similarly significant effects;
4. Systematically monitoring, tracking or observing individuals' location or behaviour.
5. Profiling individuals on a large-scale.
6. **Processing biometric data to uniquely identify an individual or enable the identification or authentication of an individual in combination with any of the other criteria set out in the WP29 DPIA Guidelines**.
7. Processing genetic data in combination with any of the other criteria set out in WP29 DPIA Guidelines.
8. Indirectly sourcing personal data where GDPR transparency requirements are not being met, including when relying on exemptions based on impossibility or disproportionate effort.
9. Combining, linking or cross-referencing separate datasets where such linking significantly contributes to or is used for profiling or behavioural analysis of individuals, particularly where the data sets are combined from different sources where processing was/is carried out for different purposes or by different controllers.
10. Large scale processing of personal data where the Data Protection Act 2018 requires "*suitable and specific measures"* to be taken in order to safeguard the fundamental rights and freedoms of individuals.

You will see that biometric data processing is at number 6 so your Employer should have carried out a DPIA and you can ask for a copy.

In my opinion that DPIA should conclude that they should offer an alternative to its employees or at the very least an option to its use.

Other recent news from around the world

German car sector receiving scrutiny

Recently the data protection authority of North Rhine – Westphalia in Germany has brought the matter into sharp focus into an investigation into the car industry.
It pointed at the following: –

1. Vehicle data can be considered personal data if it can be linked to the customer's name, or to a vehicle identification number;

2. Data processing by the garage necessary for repair, service and maintenance including data transmission to the manufacturer is legitimate where that is necessary for the purpose of fulfilling a contract to which the data subject is party, but even in such circumstances the exact nature of the processing must be made clear to the data subject. The recommendation was that this be done at the time of the order, in an addendum to the order documents;

3. The data protection authority was more sceptical of transmission of personal data to the manufacturers. In particular, it formed the view that the garages and the manufacturers were possibly both joint controllers of the personal data;

It seems that the automotive industry is now becoming a focus for data protection, and that the data protection commission here will be aware of this German investigation, as there is a regular formal coordination process between all of the data protection authorities in the EU. You can expect that the DPC will be considering launching its own investigation, now that a large proportion of the work involved has already been done in Germany.

Belgian Loyalty cards ruling

In Belgium an interesting Judgement was given by the Belgian Data Protection Authority in relation to Loyalty cards.

https://www.gegevensbeschermingsautoriteit.be/nieuws/GBA-sanctioneert-een-handelaar-voor-het-gebruik-van-de-eid-om-klantenkaart-aan-te-maken

It was ruled that asking to read an electronic ID card as a condition for the provision of a service (issuing a rewards/loyalty card) is disproportionate and in violation of GDPR. The company was fined EUR 10,000.

What you should learn from this:

- Information you collect to identify an individual needs to be proportionate to the purpose for which it is used.

- Reading and use of all data from the electronic identity card which contains name, first name, address, etc., but also the photo and the barcode that is linked to the National Register number - is excessive and disproportionate for the purpose of a commercial service (like issuing a loyalty card)
- To be valid as a legal basis, consent needs to be freely given. If no other option is provided - this is not freely given.
- In this case if the customer refused to allow his electronic id card to be used, he/she would be penalized and will not be able to enjoy the benefits and discounts because he/she would not be offered an alternative

Breaking news in Ireland

We explained in our August Newsletter that the State has been told it must delete data held on 3.2 million citizens, which was gathered as part of the roll-out of the Public Services Card, as there is no lawful basis for retaining it.

In a report on its investigation into the card, the Data Protection Commission found there was no legal reason to make individuals obtain the card in order to access State services such as renewing a driving licence or applying for a college grant.

While the card will still be sought from people accessing some services directly administered by the Department of Social Protection, the DPC has directed that the department cease processing applications for cards needed for such functions.

https://www.dataprotection.ie/en/dpc-statement-matters-pertaining-public-services-card

Then the Minister said she was going to challenge the findings and also not publish the report . But now the report is published see :

https://www.welfare.ie/en/downloads/pr170919.pdf

We will now have to await for the Appeal/JR. but it seems to me that the Department will have difficult mounting a successful judicial review of the findings, which appear to me and many others as well founded and sensible.

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.
How do you ascertain ways you might be transferring data to a UK-based company

- 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.

Advice Section - Cookies

The ePrivacy legislation does not define “consent” and it is the GDPR standard of consent that must be obtained before placing cookies on users’ devices. Users must take clear and positive action to give their consent to cookies, and continuing to use the website does not constitute valid consent.

Every day there are new products emerging, and in my opinion, one of the best is Baycloud, I have spoken to their founder and their solution is definitely worth a look.