WINTERHAWK

Helping you prepare for GDPR
One step at a time

What is Personal Data?

Legal jargon aside, the GDPR regulations helpfully outline everything you could ever want to know about Data Protection, and how any entity working with the Personal Data of EU citizens needs to incorporate them into their policies. Less helpfully, they fail to include a comprehensive list of exactly what constitutes Personal Data, not to mention Sensitive Personal Data (more on that later). Advisory group The Article 29 Working Party has provided some guidelines on the matter to steer us down the right path - but no comprehensive list. Could this be an intentional oversight, and if so, why?

One of the best single sentences describing Personal Data comes from the Article 29 WP, which defines it as *any information relating to an identified or identifiable natural person*. They have intentionally left the door wide open to interpretation, and that's the point: when trying to determine whether data is potentially of a personal nature, you have to understand the specifics of the data and apply context to it.

The above definition is actually made of four building blocks, each with a longer interpretation:

Any information

Intentionally written to be interpreted broadly. Many types of information are obvious (names, phone number, national ID numbers, etc.), but religious affiliation, gender identification, biometric data like fingerprints, dental records or even DNA could also be included. Your profile captured on CCTV could be considered personal data. An opinion formally stored as a part of an employee evaluation could be considered personal data. The new regulations have also been modernised to include items such as IP addresses and even cookie information, while still leaving room for any future developments we haven't yet envisioned.

Relating to

Is the data in question *about* a particular Data Subject? Can it be *linked* to that subject in any way? An example given by the Article 29 Working Party is the value of your house: if that value can be linked to you and can lead someone to draw conclusions or make assumptions about you (i.e. your salary, the taxes you probably owe, etc.), then it can be considered personal data.

An identified or identifiable

Often, this is something as simple as a person's name. If you run a news report stating all manner of facts and opinions about a Data Subject and you use the subject's name, that is data that has been clearly identified. Likewise, if you provide enough facts about a person (such as their address, gender and age) but do not actually name them, and if that combined information could lead back to the Data Subject, then that is identifiable data. Sometimes we try to keep data anonymous or even coded/encrypted, but if there is a way to unlock that data and link it to a person, then that also qualifies as identifiable data.

Natural person

There are certain scenarios where the deceased or unborn children are given a certain amount of protection (i.e., where data may strongly indicate information about a living person - hereditary diseases, for example), but for most purposes we can apply the standard definition of a living, breathing human being. Fictional characters need not apply.

The Article 29 Working Party appears to have fallen short of providing a concise list, but what they have done instead is possibly of greater value – they've given us a definition that we can use as a tool to form our own decisions about what is and is not personal data. Had we been given a finite list, a multitude of omitted or overlooked items would have been found, and the regulations would have lost their power.

Sensitive Data

So why make a distinction for types of data that are sensitive if we don't have a definitive list of what constitutes personal data? Simply put, certain types of data are particularly sensitive, and common sense tells us that extra care must be taken. Article 10 of the new legislation (Processing of Special Categories of Personal Data) outlines some clear examples of what can be considered sensitive.

- Racial/ethnic data
- Religious or political affiliation
- Trade Union membership
- Genetic or other biometric data
- Health or medical information
- Gender identity and/or sexual orientation
- Criminal records
- Behavioural history
- Other private data directly related to an individual

Remember, these are not exhaustive lists – GDPR legislation is not trying to draw clear lines around these definitions. We need to pay particular attention to certain kinds of sensitive data because, as Data Controllers and Data Processors, we now have even stricter obligations in regards to acquiring or processing such data. Concepts such as "Explicit Consent" or other allowances for using data in the vital interest of the Data Subject come into play (there are 11 conditions for processing this kind of data). It follows that breaches related to these categories will be considered more severe, and thus penalised more harshly. The best rule of thumb here (and really, with any personal data) is this:

If you do not need data for a specific, lawful purpose, then do not collect it in the first place.
If you do not have a specific, lawful use for data that you hold, then discard it in a safe manner.

Throughout this article, we have given a number of examples of Personal Data, but the most important point to take away is that there never can be or ever will be a final, comprehensive list. One of the key purposes of the GDPR regulation is to update existing regulations by building on them, while avoiding restrictive definitions that make the regulations irrelevant when new technologies and social issues emerge. GDPR provides us with tools to improve our understanding and implement intelligent policies and procedures. It requires us to identify Data Protection Officers who must become experts on these subjects. It requires us to perform Privacy Impact Assessments, analysing our IT infrastructure, determining where our data exists and how we must treat it. It will bring more audits from the Data Protection Authorities to determine our compliance and threatens stiffer penalties for non-compliance.

For more information about preparing for GDPR contact Winterhawk:

Email: **info@winterhawk.com**

Website **http://www.winterhawk.com/**

LinkedIn **Winterhawk EMEA & APAC**

Twitter **@WH_Global**