# Definitions

* Data privacy
* Consent
* Personal data
* (Data) Processing
* Regulation vs. directive in the EU

# Objectives

* control: opt in and provide revokable consent to how personal data is used and processed
* trust
* simplicity

# GDPR responsibilities

* Data controller / data owner: has accountability over the safety of the data – beleegyezéssel használja, csak arra használja, amire beleegyezést kapott, biztonságban tartja
* Data processor: processes data on behalf of the controller. Csak a controller utasításai szerint jár el, az ő felelőssége is az adatok védelme

Ennek az értelmezésén lehet gondolkodni. Egy lehetséges értelmezés szerint a megbízó cég a controller, és a webporta a processor.

* Data protection officer

Data controller responsibilities (Article 24):

* has appropiate measures in place
* understand the data being processed (what they have and why? what would happen if they lost that data?)

Data processor responsibilities (Article 28)

* implement security measures
* use subprocessors with the controller’s prior consent (pl. megegyezünk, hogy MySQL-t használunk, és azt oda telepítjük, ahová a kedves vevő kívánja (felhő vagy on-premise). Lényeges, hogy az adatoknak EU-n belül kell maradnia.
* contracts with the controller
* process only data in scope. Logs processing activities(!!!)

Storage:

* how and where data is stored
* how is it protected? (Ha felhőben van, milyen írásos garanciáink vannak az adatbiztonságra?)
* how is data encrypted?
* how access is managed?

Reporting:

* logging, monitoring, managing and reporting activity on data

# Requirements

GDPR basis of processing data

* consent (önkéntes és visszavonható). Ide tartozik az is, hogy új beleegyezés kell, ha valami változik. Tehát tárolni kell a beleegyezés tényét, de lehet, hogy az időpontját is. El lehet azon gondolkodni, hogy legyen-e adatmódosítás címén egy olyan összetett felület, ahol az adatok kezelésének köre le vannak írva, vagy legalábbis tájékozódni lehet róluk további linkeken.
* contarctual necessity
* legal obligation
* protect vital interest
* legitimate interest
* public interest (pl. járvány idején közérdek lehet bizonyos személyes adatok összegyűjtése)

Technical measures (Article 32)

* data in transit: TLS
* data at rest: AES256
* ability to restore
* regular testing and evaluation

Notification in case of a breach

* ha a természetes személy adatai veszélyben lehetnek, őt mindenképpen értesíteni kell (pl. felhívás jelszóváltoztatásra egy jó ötlet lehet)
* a processor a controllert értesíti
* nature of the breach: number of people and records
* likely consequences
* proposed mitigation
* must notify plainly and not in technical language

# Data subject rights

* Right of access (Article 15): access on request, freely (kivéve ha túl sokszor kéri)
* Right to correction (Article 16). Amennyiben a pontatlan / hiányos információ harmadik fél számára is rendelkezésre lett bocsátva, őt is tovább kell értesíteni
* Right to be forgotten (Article 17). A törlés akkor kérhető, ha nincs már jogi alapja az adatkezelésnek. Tehát ha az adatkezelés kizárólag beleegyezésre történt, az bármikor visszavonható, és akkor törölni kell. De ugyanúgy törölni kell pl. az elévült adatot (pl. ha a munkáltatónak már nem kell tovább őriznie az adott dokumentumot)
* Right to object: ez minket annyira nem érint. De pl. marketing célú hozzájárulás szokott ilyen lenni
* Children under 16 – ez se annyira releváns
* Portability: kérésre importálható (pl. SQL kód) módon is rendelkezésre kell tudnunk bocsátani az adatokat.
* Prompt response: ált. 30 nap. Ami azt jelenti, hogy adott esetben elég kézzel dolgozni. De ha meg lehet csinálni, érdemes automatizálni.

# Breach notification

Itt inkább az a kérdés, hogy hogyan észlelünk egy ilyet. A webporta feladata inkább az ügyfél mihamarabbi értesítése.

# Adatbiztonság

Alapkövetelmény az adatok biztonságos tárolása és kezelése. Tudunk-e valamilyen titkosítást használni az adatbázisban, vagy maga az adatbázis erre már egyfajta garancia?

Csak azért nem gyűjtünk be semmilyen adatot, mert hátha még jó lesz. Minimalizálnunk kell. Másrészt, ha van egy új ötlet, arra a meglévő adatokat csak beleegyezés után használhatjuk fel.

# Egyéb ötletek

Csak Magyarországról elérhető oldal?

Monitorozzuk és dezaktiváljuk a 60 napnál régebben nem használt felhasználói fiókokat. Ezeket csak az adminisztrátor fogja tudni helyreállítani. (Kérdés, ki állítja helyre az adminisztrátort? De feltételezhetjük, hogy az összes adminisztrátor csak nem lesz inaktív.)