



# Personas datu aizsardzības aspekti informācijas tehnoloģijās

---

Agnese Boboviča, CIPP/E  
Personas datu aizsardzības speciāliste



Personas da



jeb  
vai mēs mākam izstāstīt (tā lai viņa saprot!!!!)

vecmammai

KĀ un kāpēc DARBOJAS:

whatsapp,

facebook,

HR sistēma ABC,

grāmatvedības uzskaites sistēma YWZ,

.....

cijas

Agnese Boboviča, CIPP/E

Personas datu aizsardzības speciāliste




# UZZIŅAI....

- Fizisko personu datu aizsardzības likums;
- MK noteikumi Nr.216: Kārtība, kādā sagatavo un iesniedz personas datu apstrādes atbilstības novērtējumu;
- MK noteikumi Nr.40: Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības;

- 27.04.2016. EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (vispārīgā datu aizsardzības regula)

piemērošana no 25.05.2018., spēkā jau TAGAD!





**"personas dati"** ir jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu ("datu subjekts");  
identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem;

Sensitīvi dati:

---

FPDAL: Personas dati, kas norāda personas rasi, etnisko izcelsmi, reliģisko, filozofisko un politisko pārliecību, dalību arodbiedrībās, kā arī sniedz informāciju par personas veselību vai seksuālo dzīvi.

REGULA:

9.pants

Īpašu kategoriju personas datu apstrāde

1. Ir aizliegta tādu personas datu apstrāde, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, un ģenētisko datu, biometrisko datu, lai veiktu fiziskas personas unikālu identifikāciju, veselības datu vai datu par fiziskas personas dzimumdzīvi vai seksuālo orientāciju apstrāde.

Pseidonimizācija ir identitātes maskēšanas process. Procesa efektivitāte ir atkarīga no informācijas apstrādes procesa, atpakaļizsekojamības, cik liela ir datu kopa, kurā ir "paslēpt" indivīds, u.tml.

REGULA: "pseidonimizācija" ir personas datu apstrāde, ko veic tādā veidā, lai personas datus vairs nav iespējams saistīt ar konkrētu datu subjektu bez papildu informācijas izmantošanas, ar noteikumu, ka šāda papildu informācija tiek turēta atsevišķi un tai piemēro tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka personas dati netiek saistīti ar identificētu vai identificējamu fizisku personu;

### Anonīmi dati:

Anonīmi dati ir tādi dati, kas attiecas uz fizisku personu, ja šo personu nevar identificēt ne datu pārzīnīs, ne kāda cita persona...nemot vērā visus līdzekļus, kurus, iespējams, pamatoti izmantotu vai nu personas datu pārzīnīs, vai jebkura cita persona, lai identificētu minēto personu.

Personas identifikācija ne pie kādiem apstākļiem NAV IESPĒJAMA!



# Regulas 76

## apsvērumis:

Riska iespējamība un nopietnība attiecībā uz datu subjekta tiesībām un brīvībām būtu jānosaka, atsaucoties uz apstrādes raksturu, piemērošanas jomu, kontekstu un nolūku. Risks būtu jāizvērtē, pamatojoties uz objektīvu novērtējumu, ar ko nosaka, vai datu apstrādes darbības ietver risku vai augstu risku.



# Regulas 84

## apsvērumus:

Lai sekmētu šīs regulas noteikumu ievērošanu gadījumos, kad apstrādes darbības varētu izraisīt augstu risku fizisku personu tiesībām un brīvībām, pārzinīm vajadzētu būt atbildīgam par novērtējuma par ietekmi uz datu aizsardzību veikšanu, lai jo īpaši izvērtētu minētā riska avotus, raksturu, specifiku un nopietnību. Novērtējuma rezultāti būtu jāņem vērā, nosakot piemērotus pasākumus, kas veicami, lai uzskatāmi parādītu, ka personas datu apstrāde atbilst šai regulai....





(75) Risku fizisku personu tiesībām un brīvībām - ar atšķirīgu iespējamību un nopietnību - var radīt personas datu apstrāde, kas var izraisīt fizisku, materiālu vai nemateriālu kaitējumu, jo īpaši, ja apstrāde var izraisīt diskrimināciju, identitātes zādzību vai viltošanu, finansiālu zaudējumu, kaitējumu reputācijai, ar dienesta noslēpumu aizsargātu personas datu konfidencialitātes zaudēšanu, neatļautu pseidonimizācijas atcelšanu vai jebkādu citu īpaši nelabvēlīgu ekonomisko vai sociālo situāciju; ja datu subjektiem var tikt atņemtas viņu tiesības un brīvības vai atņemta

iespeja kontrolēt savus personas datus;

ja tiek apstrādāti personas dati, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību, piederību arodbiedrībai, un ja tiek apstrādāti ģenētiskie dati, veselības dati vai dati par dzimumdzīvi, vai sodāmību un pārkāpumiem vai ar tiem saistītiem drošības pasākumiem; ja tiek izvērtēti personiskie aspekti, jo īpaši analizējot vai prognozējot aspektus attiecībā uz personas sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm vai interesēm, uzticamību vai uzvedību, atrašanās vietu vai pārvietošanos, lai izveidotu vai izmantotu personiskos profilus; ja tiek apstrādāti neaizsargātu fizisku personu, īpaši bērnu, personas dati; vai ja apstrāde ietver lielu personas datu daudzumu un ietekmē lielu skaitu datu subjektu.



## FPDAL 26.2:

(2) valsts un pašvaldības institūcijas un privātpersonas, kurām deleģēti pārvaldes uzdevumi, sagatavo personas datu apstrādes atbilstības novērtējumu, ietverot tajā arī riska analīzi un pārskatu par informācijas drošības jomā veiktajiem pasākumiem.

## MK Nr. 216:

Noteikumi attiecas uz valsts un pašvaldību institūcijām un privātpersonām, kurām deleģēti valsts pārvaldes uzdevumi (turpmāk – iestāde).



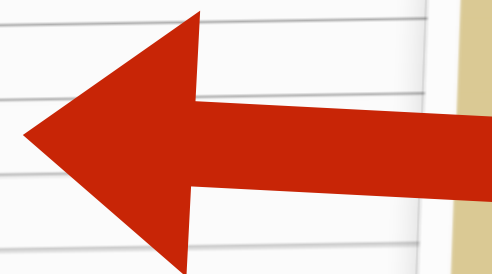
## Ministru kabineta noteikumi Nr. 40

Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības:

.....

6. Datu apstrādē ieviesto tehnisko un organizatorisko prasību novērtējumu pārzinis sagatavo normatīvajā aktā par personas datu apstrādes atbilstības novērtējuma izstrādes un iesniegšanas kārtību noteiktajos gadījumos.

Datu apstrādē ieviesto tehnisko un organizatorisko prasību novērtējumā pārzinis norāda informāciju vismaz tādā apmērā, kāds noteikts normatīvajos aktos par personas datu apstrādes atbilstības novērtējuma izstrādes un iesniegšanas kārtību



# Novērtējumu sagatavo:

1. pirms personas datu apstrādes uzsākšanas jaunam personas datu apstrādes mērķim;
2. pirms tādu izmaiņu veikšanas personas datu apstrādē, kas ietekmē datu subjekta tiesības vai intereses personas datu aizsardzības jomā;
3. pēc iestādes iniciatīvas;
4. pēc Datu valsts inspekcijas pieprasījuma.



katram datu apstrādes  
mērķim sagatavojams  
atsevišķs novērtējums/  
analīze!!!



Jāspēj pamatot kāpēc tieši tādu datu kategorija ir iekļauta datu bāzē, ko ar to informāciju darīs!!!

1. kāds ir personas datu apstrādes mērķis?

2. Vai personas datu apstrādes mērķi nosaka normatīvie akti? Ja jā, norādīt normatīvos aktus, kas paredz datu apstrādi.

3. Kādi personas datu veidi, piemēram, vārds, uzvārds, personas kods, tiek apstrādāti, lai sasniegtu iepriekšējā punktā norādīto mērķi?

4. Ja tiek apstrādāti sensitīvie personas dati, norādiet sensitīvo personas datu veidus, kas tiek apstrādāti.

5. Kādā veidā notiek personas datu apstrāde – manuāli vai automatizēti?

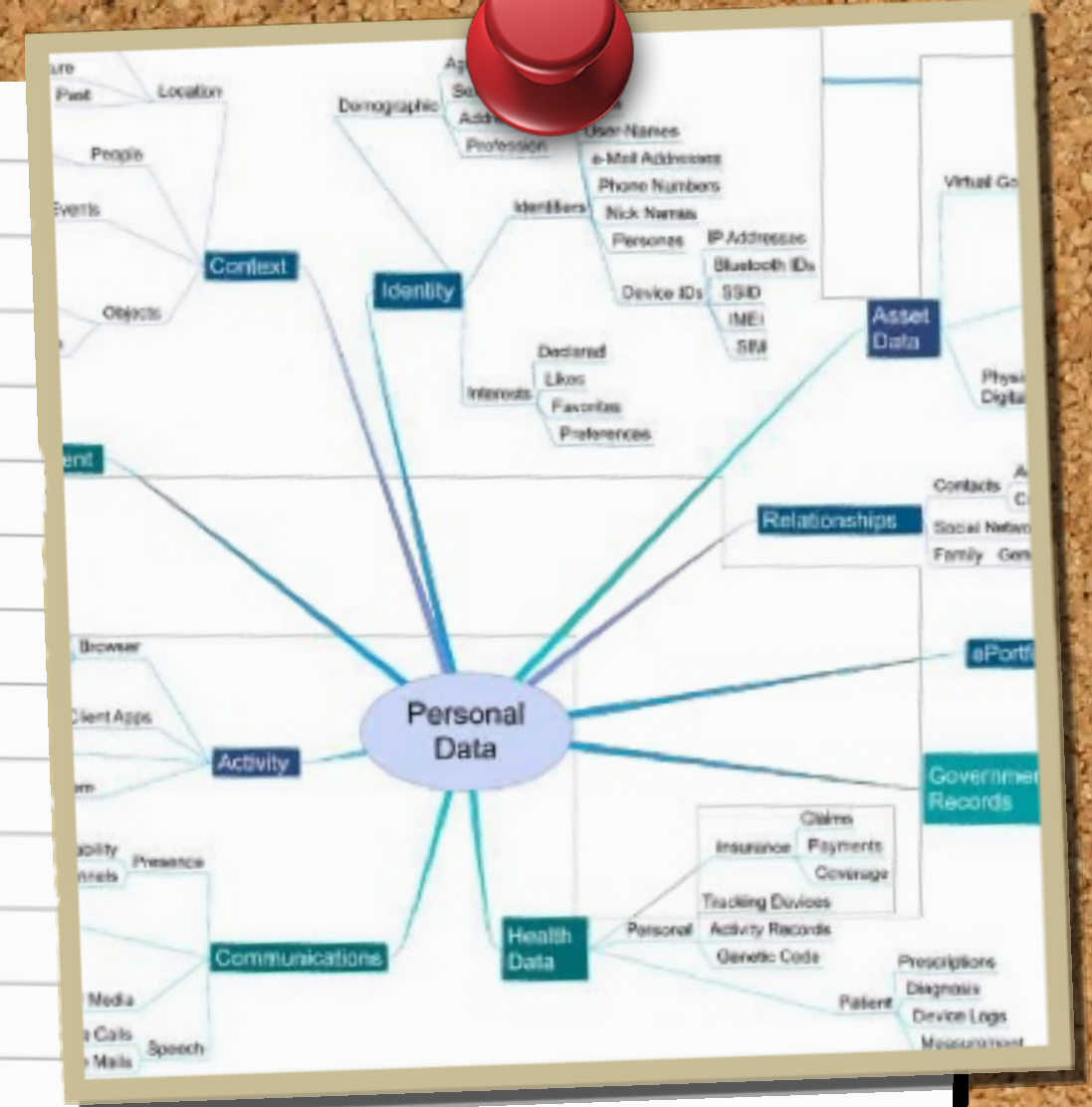
6. Vai sensitīvo personas datu apstrāde ir nodalīta vai diferencēta no pārējo personas datu apstrādes? Ja jā, raksturojiet procedūru, kā tas ir nodrošināts. Ja nē, norādiet iemeslus.



7. Vai ir apzināti visi personas dati, kas ir nepieciešami personas datu apstrādes mērķa sasniegšanai? Ja jā, uzskaitiet šos datus, norādot, kādēļ tie nepieciešami personas datu apstrādes mērķa sasniegšanai. Ja nē, norādiet iemeslus.

8. Vai personas datu apstrādes mērķi var sasniegt, neapstrādājot vispār personas datus vai apstrādājot mazākā apjomā? Pamatojiet.

9. Norādiet personas datu apstrādes tiesisko pamatu atbilstoši Fizisko personu datu aizsardzības likuma 7. pantam. Ja tiek apstrādāti sensitīvie personas dati, norādiet pamatojumu atbilstoši Fizisko personu datu aizsardzības likuma 11. pantam

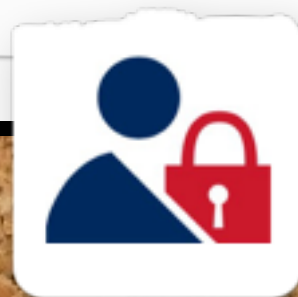


10. Ja personas datu apstrādes tiesiskais pamats ir datu subjekta **piekrišana (!!!!)**, norādiet, kādā veidā (elektroniski, rakstiski, mutiski) un kurā brīdī tiek iegūta datu subjekta piekrišana?

11. Ja sensitīvie personas dati tiek apstrādāti, pamatojoties uz datu subjekta piekrišanu, norādiet, vai šī piekrišana tiek noformēta rakstveidā. Ja nē, pamatojiet, kāpēc datu subjekta piekrišana netiek noformēta rakstiski.

12. Vai personas datu apstrāde ir uzticēta **personas datu operatoram**? Ja jā, norādiet, tiesisko pamatu.

13. Vai personas datu apstrāde ir reģistrēta Datu valsts inspekcijā? Ja nē, norādiet pamatojumu.



...SYSTEM IS  
...ACCURATE....AS  
...LONG AS THE CLIENT  
IS CALLED COLIN AND  
LIVES IN SWINDON

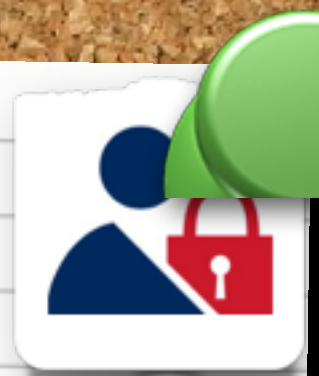


### Delete "WhatsApp"?

Deleting this app will also delete its data, but any documents or data stored in iCloud will not be deleted.

Delete

Cancel



11. Rīska analīze attiecībā uz personas datu subjekta tiesībām un brīvībām:

1. Personas datu apstrāde atbilstoši personas datu apstrādes mērķim
2. Adekvāta personas datu apstrāde
3. Personas datu **glabāšana** atbilstoši personas datu apstrādes **mērķim**
4. Personas datu izpaušana

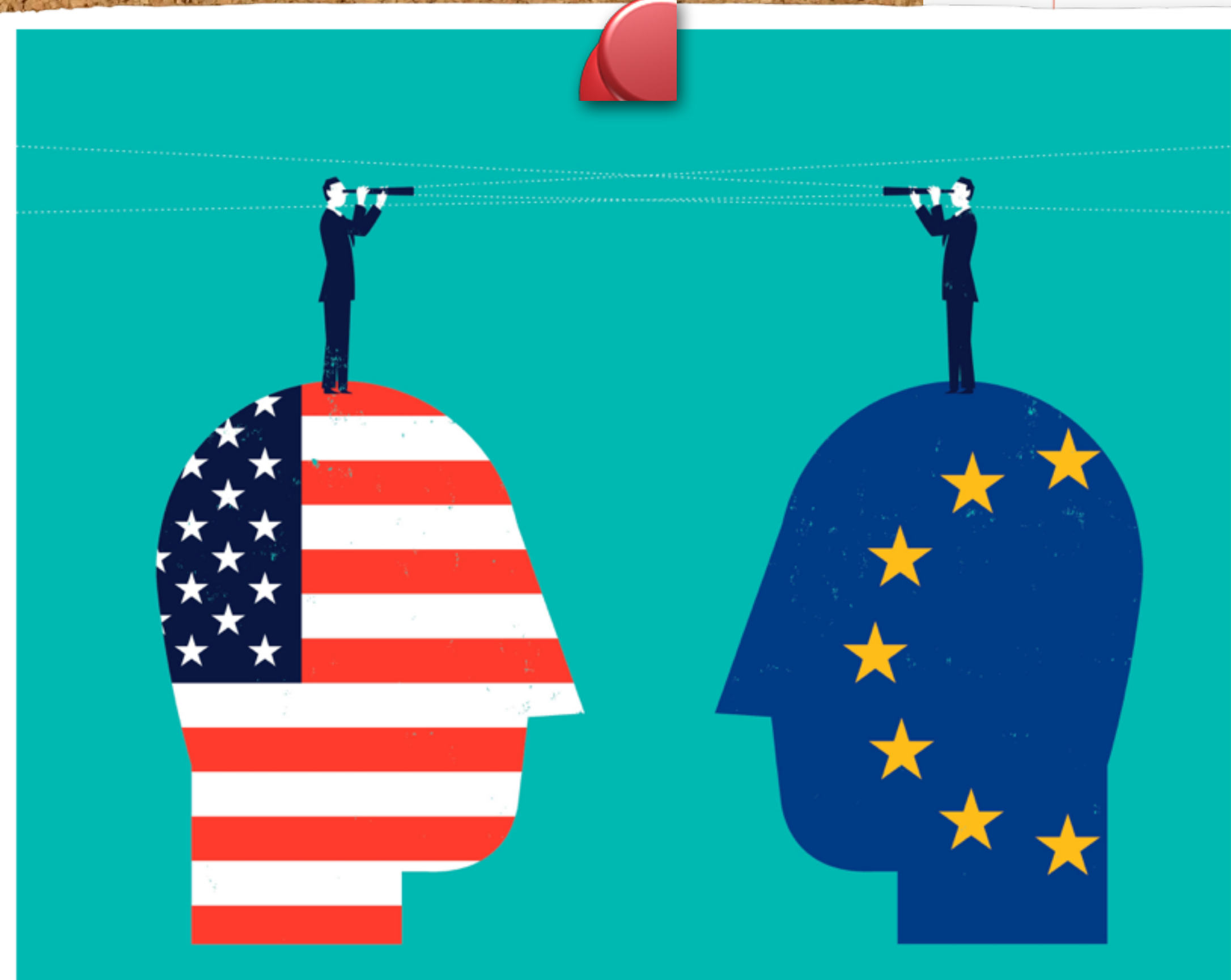
## 5. Datu subjekta tiesību nodrošināšana:

5.1. Datu subjekta informēšana par viņa personas datu apstrādi;

5.2. Datu subjekta tiesības piekļūt saviem personas datiem;







6. Personas datu nodošana valstīm,  
kas nav Eiropas Savienības vai  
Eiropas Ekonomikas zonas  
dalībvalstis, vai valstīm, kuras nav  
saņēmušas Komisijas atzinumu par  
adekvātu datu aizsardzības līmeni





### III. Personas datu aizsardzības un drošības pasākumi

- Vai ir izstrādāti personas datu apstrādes aizsardzības noteikumi, kas ir ieviesti pēc neautorizētas un prettiesiskas piekļuves personāliem, kas ir apstrādāti automatizēti vai manuāli;
- Vai iestādē ir izstrādātas informācijas sistēmu piekļuves kontroles procedūras? ja atbilde ir "jā", kā iestāde pārvalda informācijas sistēmu lietotāju kontus?
- Vai iestādē ir nodrošināta informācijas sistēmas notikumu reģistrēšana un monitorēšana? Raksturojiet kārtību;
- Vai iestādes informācijas sistēmām var piekļūt attālināti? ja atbilde ir "jā", kāda ir attālinātas piekļuves procedūra un nosacījumi?
- .....





PALDIES PAR UZMANĪBU!



AGNESE BOBOVIČA, CIPP/E

Personas datu aizsardzības speciāliste

[www.datuaizsardziba.lv](http://www.datuaizsardziba.lv)

Twitter: @datuaizsardziba

epasts: [info@datuaizsardziba.lv](mailto:info@datuaizsardziba.lv)

tālrunis: +371 20018311

