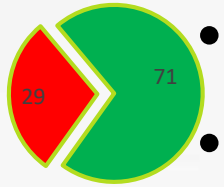
Z varstvom osebnih podatkov ne čakajte na maj

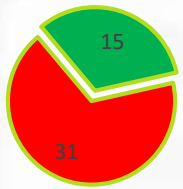
Splošna uredba o varstvu podatkov (GDPR) in upravljanje identitet

Andrej Zimšek

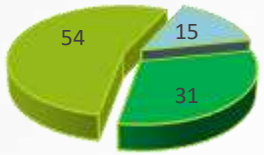
VAROVANJE OSEBNIH PODATKOV - STANJE



- 71% meni da mora razkriti osebne podatke za dostop do storitev
- 70% meni da bodo podatki zlorabljeni
- 69% bi rado dalo izrecno dovoljenje za obdelavo osebnih podatkov



- 15% meni da ima nadzor nad osebnimi podatki
- 31% meni da sploh nima nadzora nad osebnimi podatki
- 37% se zaveda obstoja organa pristojnega za varovanje osebnih podatkov



- Vsi želijo biti obveščeni o zlorabah podatkov (kraja, izguba, …)

Posebna raziskava Eurobarometra št. 431 varstvo podatkov, junij 2015

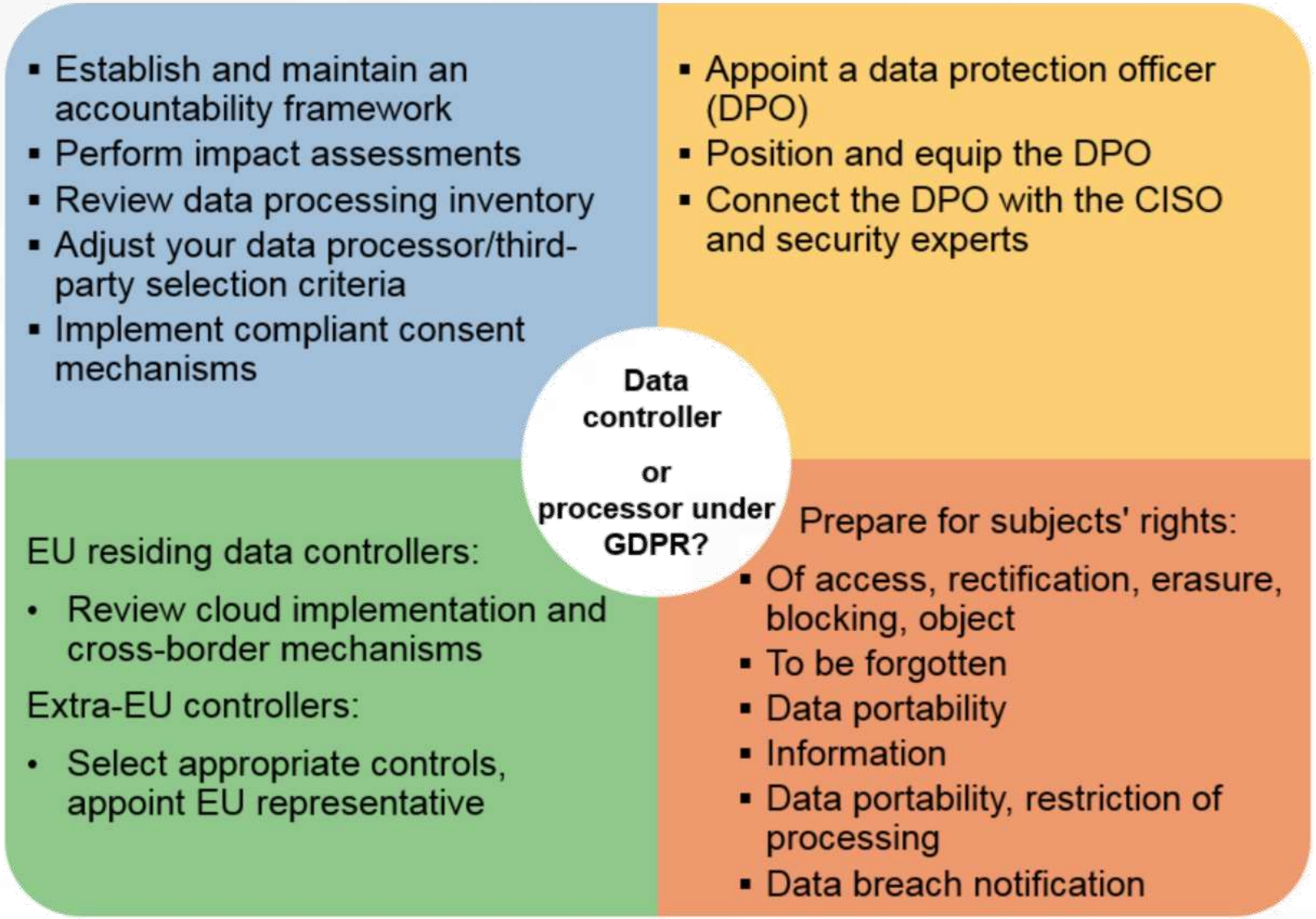
BRIHTEJA

65000 družb

1500 DPO

miljoni osebnih podatkov

SPLOŠNA UREDBA O VARSTVU PODATKOV - GDPR



Source: Gartner (September 2016)

SPLOŠNA UREDBA O VARSTVU PODATKOV

- Potrebna je neposredna odobritev pred obdelavo osebnih podatkov
- Specifikacija pravic uporabnikov
  - Področje uporabe
  - Čas hranjenja
  - Mesto hranjenja podatkov
  - …
- Obravnavanje tveganj povezanih z obdelavo osebnih podatkov
- Kdo upravlja, Kdo ima dostop do podatkov
- Odstranjevanje vseh „nepotrebnih“ podatkov

GDPR – PRAVICE POSAMEZNIKA

- Pravica do pozabe
- Prenosljivost podatkov

- Obveščanje o varnostnih tveganjih (72 ur)
  - Neavtorizirana uporaba
  - Razkritje
  - Odtujitev
  - Sprememba podatkov
  - Izbris podatkov

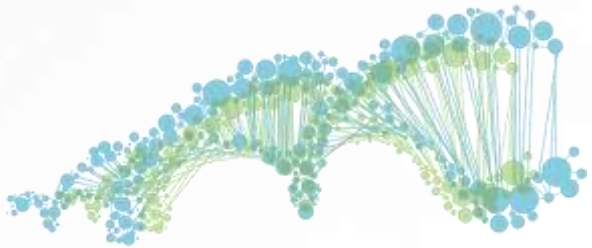
KDO

Vsa podjetja, ki obdelujejo / shranjujejo podatke državljanov evropske unije se morajo ravnati skladno z uredbo

KAJ

Vsi podatki, ki lahko enolično določijo posameznika so osebni podatki.

(IP naslov, biometrični podatki, slike, finančni podatki, podatki o lokaciji, spletni identifikator, … oz. navedba enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika)



Genetski zapis

Finančni podatki

Socialna identiteta

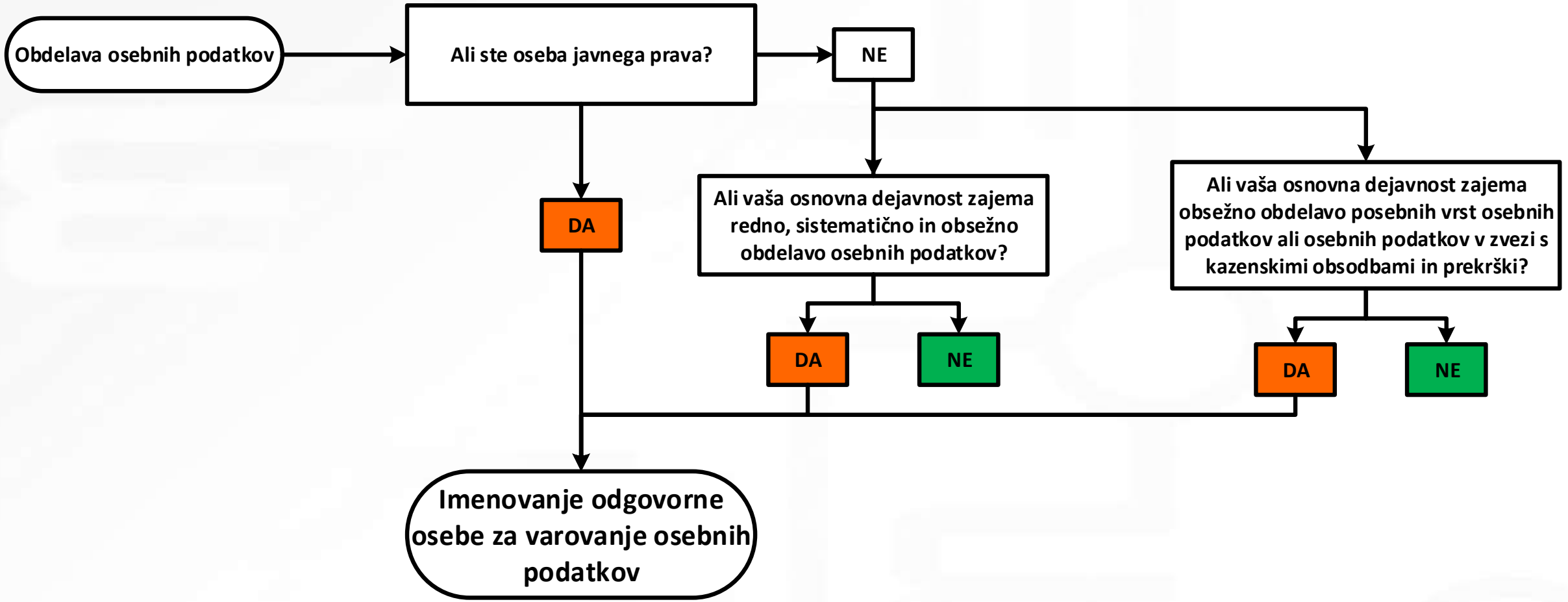
URADNA OSEBA ZA VARSTVO OSEBNIH PODATKOV

Uradna oseba za varstvo osebnih podatkov (ang. data protection officer - DPO) bo skrbela za skladnost z zakonodajo in za ustrezno varstvo osebnih podatkov. Po nekaterih ocenah jih bo Evropska unija potrebovala do 28.000 v naslednjih dveh letih, od tega Slovenija 1.500.

Predvsem za javni sektor in za zasebni sektor kjer se sistematično in obsežno spremljajo osebni podatki posameznikov (javni zavodi, banke, zavarovalnice, trgovci, …)

Pomoč pri zagotavljanju skladnosti

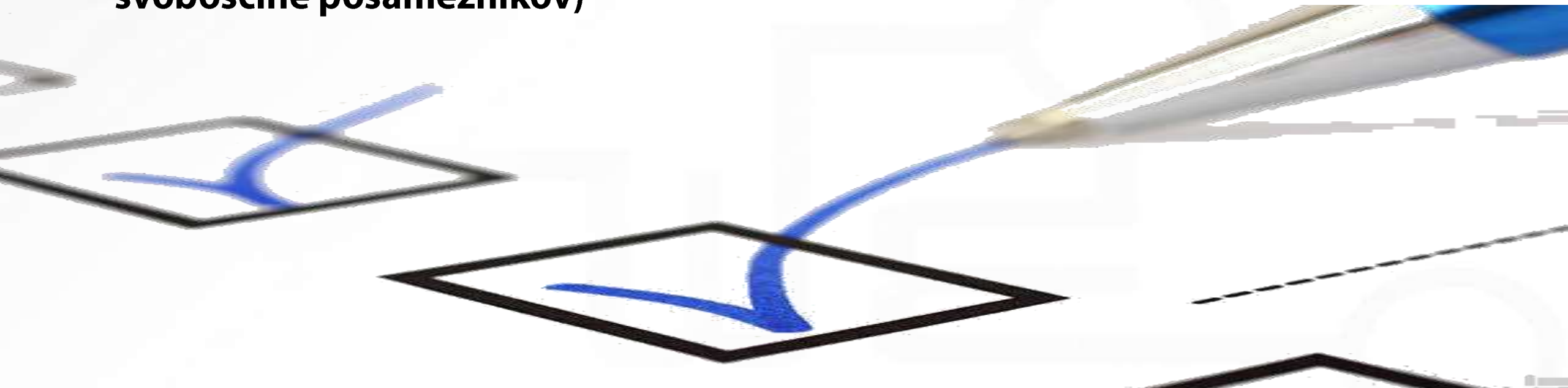
URADNA OSEBA ZA VARSTVO OSEBNIH PODATKOV



OCENA UČINKA

Ocena učinka v zvezi z varstvom podatkov

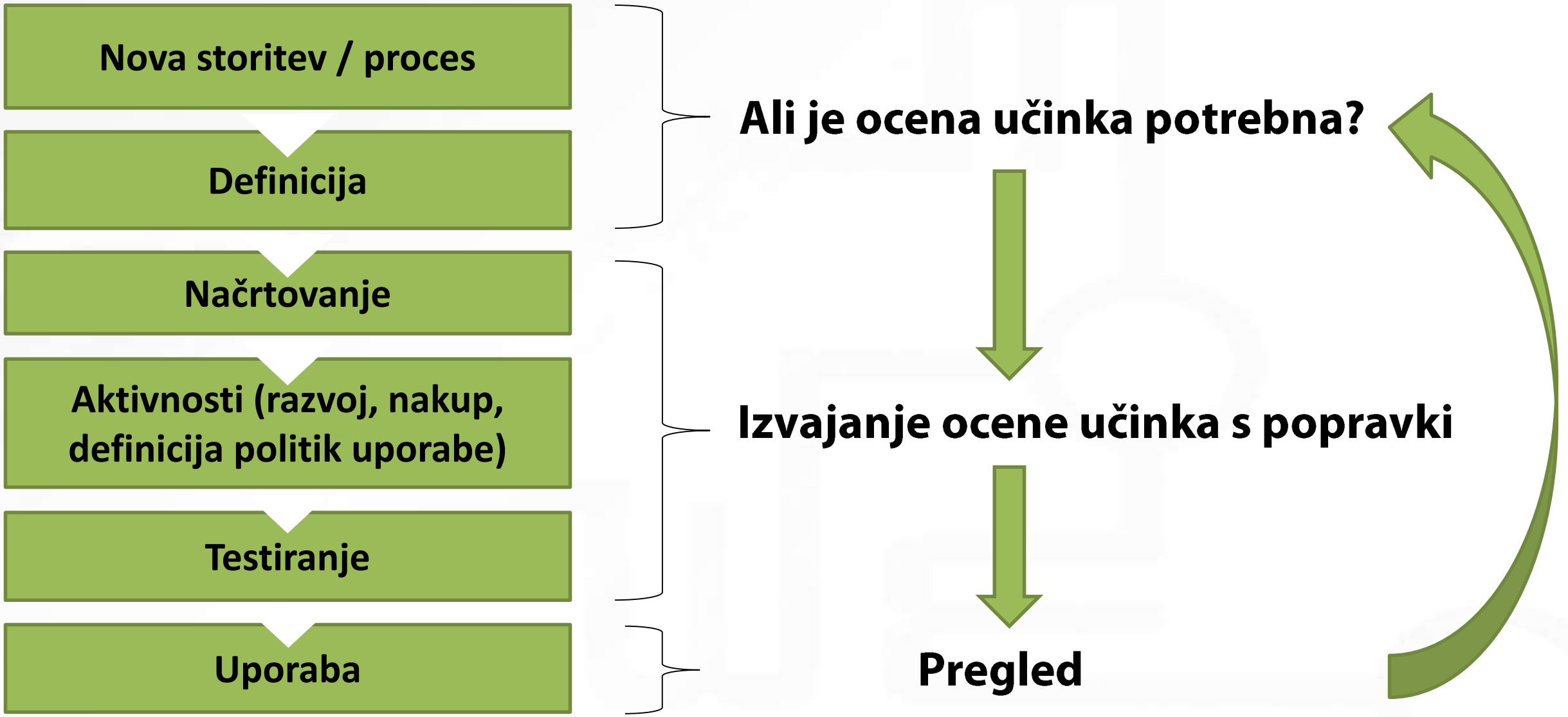
Pred uvedbo novih obdelav osebnih podatkov bo potrebno opraviti t.i. Data Protection Impact Assessment (DPIA), s čimer se bo zagotovila skladnost postopkov / rešitev z zakonodajo (veliko tveganje za pravice in svoboščine posameznikov)



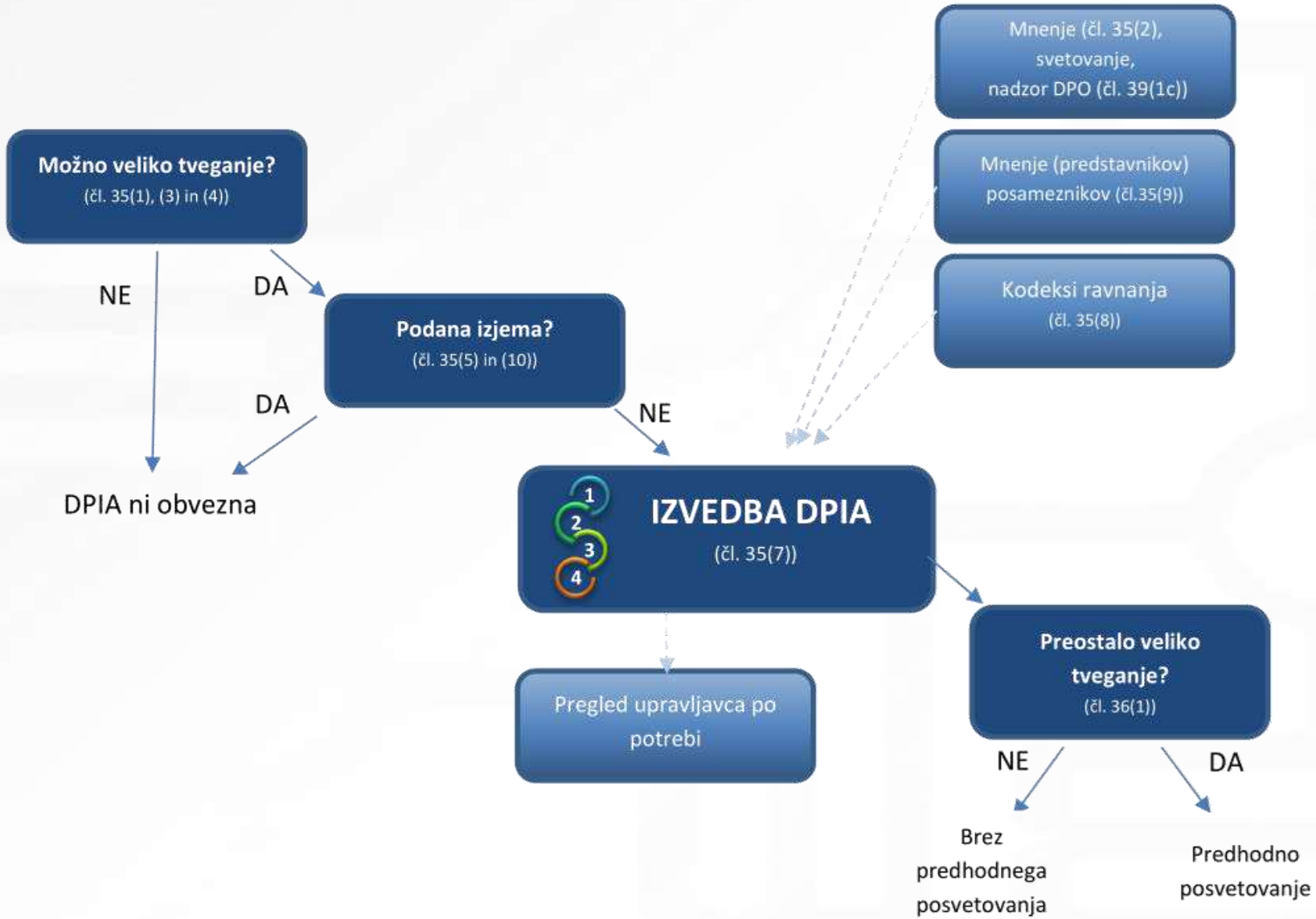
OCENA UČINKA V ZVEZI Z VARSTVOM PODATKOV

- pravočasno ugotovimo, kje bi lahko kršili zakonodajo,
- uvedemo primerne ukrepe za izogibanje in zmanjševanje tveganj,
- izkazujemo skladnost z načelom odgovornega ravnanja s podatki in
- se izognemo kršitvam zakonodaje, ki lahko vodijo v:
  - uvedbo inšpekcijskih postopkov
  - izrek upravnih glob
  - negativno medijsko poročanje
  - izgubo dobrega imena zaupanja s strani posameznikov, deležnikov in javnosti v organizacijo.

OCENA UČINKA V ZVEZI Z VARSTVOM PODATKOV



DPIA – PRIPOROČILA IP



Vir: https://www.ip-rs.si/fileadmin/user_upload/Smernice_o_ocenah_ucinka__DPIA__nov2017.pdf

VGRAJENO IN PRIVZETO VARSTVO PODATKOV

zaupnost in zasebnost vgrajena v vsak sistem in proces že v fazi planiranja

… v obdelavo vključiti potrebne zaščitne ukrepe, da se izpolnijo zahteve uredbe in zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki.

VAROVANJE OSEBNIH PODATKOV

- Kateri osebni podatki so shranjeni?
- Kdo je zadolžen za te podatke?
- Kdo lahko dostopa do podatkov?
- Kako dolgo so lahko podatki shranjeni?

- Brisanje podatkov, ki se ne uporabljajo
- Zastarane pravice za dostop do podatkov
- Zagotavljanje minimalnega dostopa do podatkov

VAROVANJE OSEBNIH PODATKOV

- Centralen pregled nad pravicami uporabnikov pri dostopu do osebnih podatkov
- Avtomatiziran pregled pravic za dostop do podatkov
- Obveščanje o spremembah pravic
- Zagotavljanje principa ločevanja nalog in dolžnosti (Segregation of Duties, Least privilege)
- Proces za dodeljevanje pravic

UPRAVLJANJE UPORABNIŠKIH IDENTITET

- Pregled vseh procesov in določitev postopkov
- Avtomatsko delovanje sistema glede na podatke iz avtoritativnih virov
- Posredovanje IT osebja ni več potrebno
- Vse pravice so določene glede na vhodne podatke oz. potrjene s strani odgovornih oseb
- Pregled vseh pravic

IDENTITETA, PROCESI, INFORMACIJE

Gartner

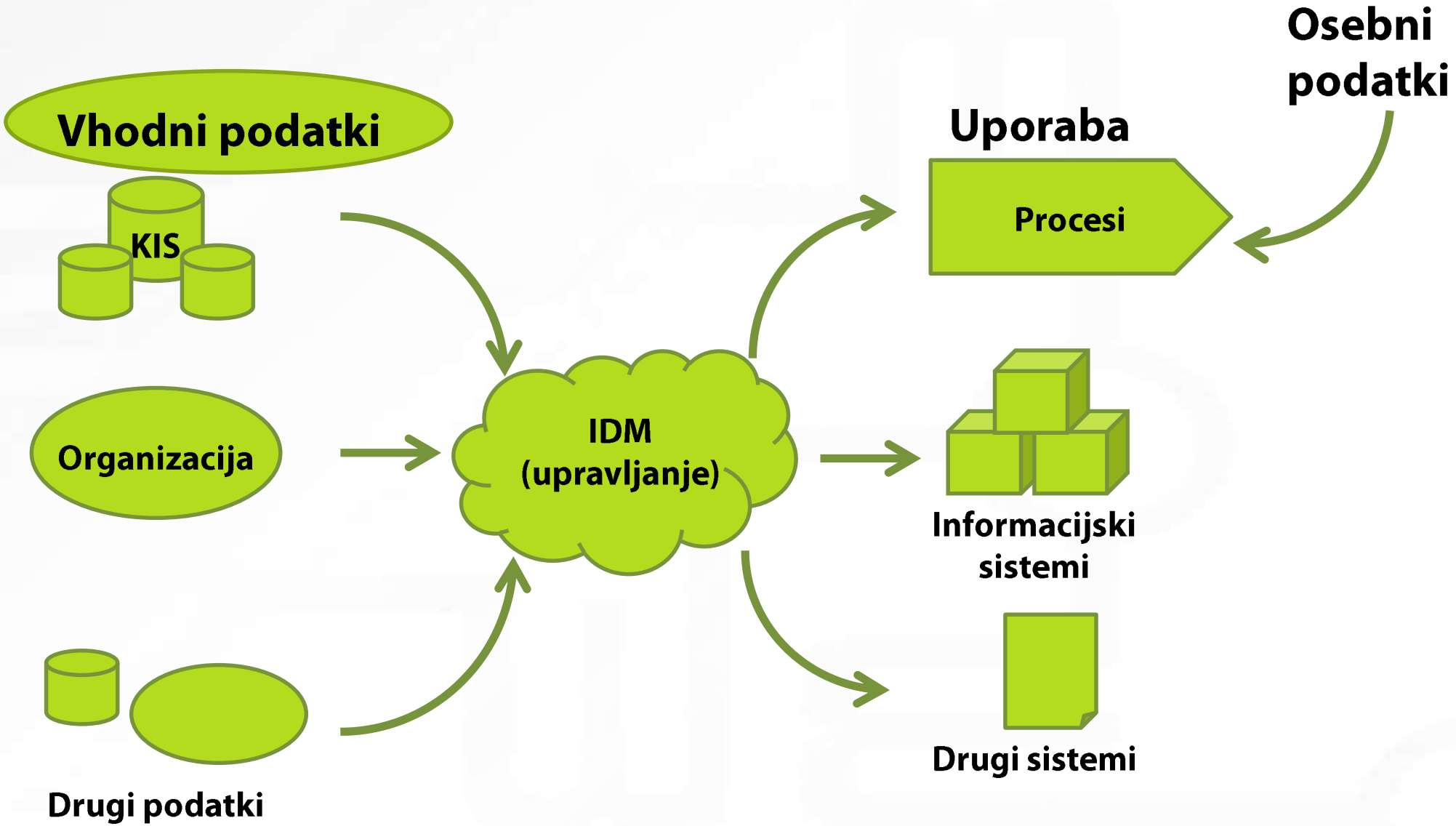
Identity and Access Management (IAM) *is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons.*

PRAVI LJUDJE

DOSTOP DO VIROV

OB PRAVEM ČASU

OSNOVNI ELEMENTI - UPRAVLJANJE IDENTITET



KAKO PRISTOPITI

1. Kje so shranjeni osebni podatki? Kateri? Namen uporabe?
2. Pregled postopkov, morebitnih privoljenj, …
3. Brisanje osebnih podatkov, ko niso več potrebni
   a) Pregled pravnih podlag
   b) Minimizacija obdelave
4. Omejevanje dostopa do osebnih podatkov
5. Preprečevanje izgube oz. spremembe osebnih podatkov
6. Poročanje - detekcija varnostnih incidentov in samoprijava…
7. Če je potrebno - DPO in DPIA (Odgovorna oseba za varovanje podatkov, Ocena učinka v zvezi z varstvom osebnih podatkov)

DOGAJA SE TUDI ….

The Guardian understands Deloitte discovered the hack in March this year (2017), but it is believed the attackers may have had access to its systems since October or November 2016.

The hacker compromised the firm's global email server through an "administrator's account" that, in theory, gave them privileged, unrestricted "access to all areas".

The account required only a single password and did not have "two-step" verification, sources said.

Emails to and from Deloitte's 244,000 staff were stored in the Azure cloud service, which was provided by Microsoft

KJE ZAČETI, DOBRE PRAKSE

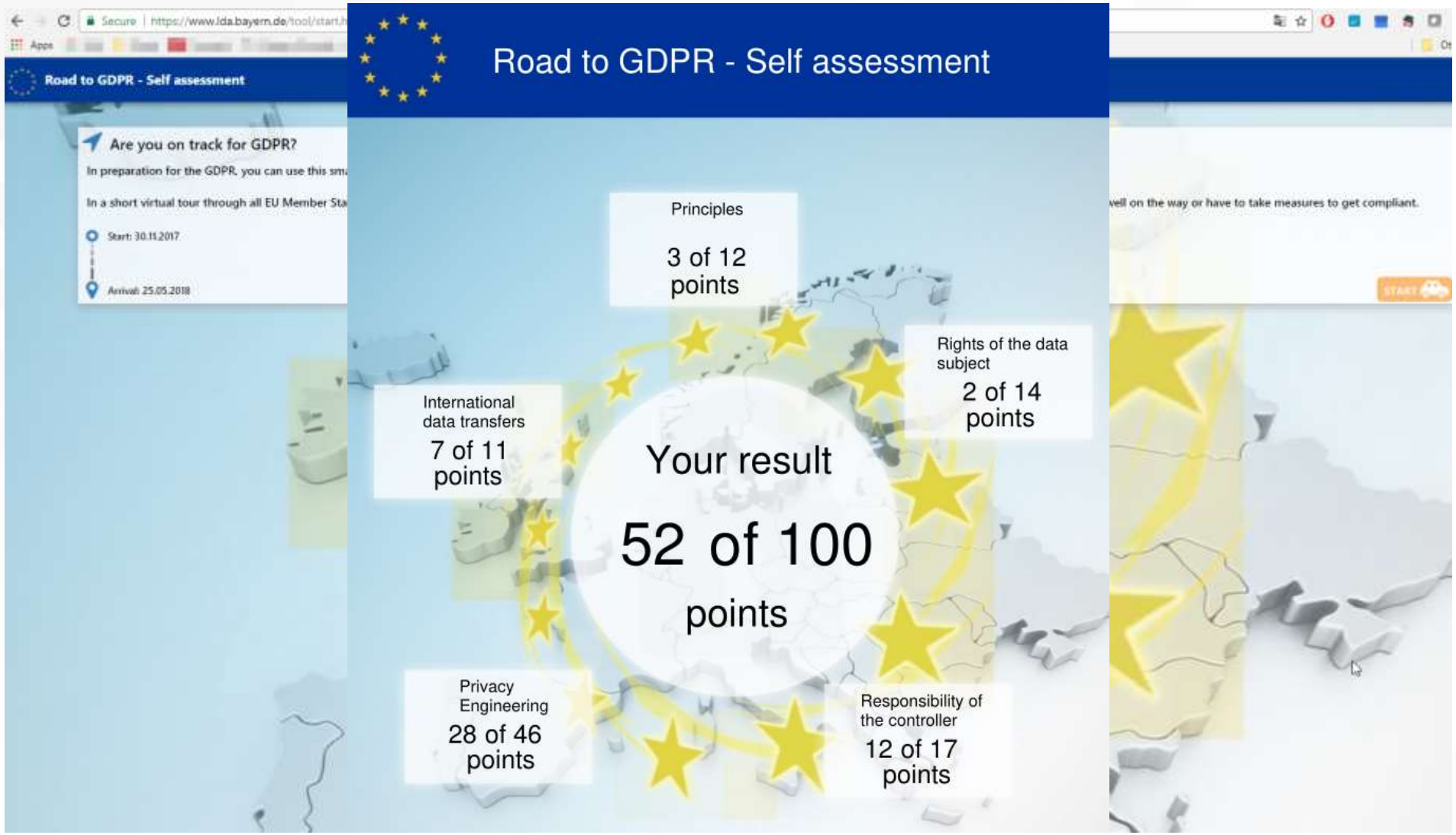
- Dodatne informacije
  - Stran informacijskega pooblaščenca
  - Ministrstvo za pravosodje – ZVOP-2
  - Uradna stran EU o uredbi GDPR

- **Google bo opozarjal na zbiranje osebnih podatkov brez privolitve uporabnika v Android aplikacijah** (Google Safe Browsing warnings)
- **Zavarovalnica Triglav :** Kaj je dobro vedeti, ko vas pokliče zavarovalnica

http://vsebovredu.triglav.si/premozenje/naj-vas-klic-zavarovalnice-ne-spravi-v-slabo-voljo

SAMOTESTIRANJE

https://www.lda.bayern.de/tool/start.html#



Hvala