

## GDPR PO GDPR

kako se je nova zakonodaja uveljavila v praksi



mag. Matjaž Drev  
državni nadzornik za varstvo osebnih podatkov

Informacijski pooblaščenec RS



## OSEBNI PODATKI, NOVA VALUTA?

1995: Direktiva 95/46/ES

2004: ZVOP-1

2018: GDPR

2019: ZVOP-2?

## (R)EVOLUCIJA?

### Kaj se (še) ni spremenilo?

- Pravna podlaga
- Pravice posameznikov
- Pogodbena obdelava
- Informacijska varnost
- Globe

### Kaj se je spremenilo?

- Samoprijave kršitev
- Pooblaščen osebe (DPO)
- Ocene učinkov (DPIA)
- Mednarodne inšpekcije
- Kodeksi, certifikati

## CEKINI PADAJO Z NEBA?

[www.enforcementtracker.com](http://www.enforcementtracker.com)

### GDPR Enforcement Tracker

This website contains a list and overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO) to keep this list as up-to-date as possible. Since not all fines are made public, this list can of course never be complete, which is why we appreciate any [indication of further GDPR fines and](#)

Country	Authority	Date	Penalty	Against	Legal basis	Summary
FRANCE	French Data Protection Authority (CNIL)	2019-01-21	30,000,000	Google Inc.	Art. 13 GDPR, Art. 14 GDPR, Art. 6 GDPR, Art. 4 nr. 11 GDPR, Art. 5 GDPR	The fine was imposed on the basis of complaints from the Austrian organisation "Name of your business" and the French NGO "La Quadrature du Net". The complainants were filed on 28th and 29th of May 2018 - immediately after the DSGVO became applicable. The complainants concerned the creation of a Google account during the configuration of a mobile phone using the Android operating system. The CNIL imposed a fine of 30 million euros for lack of transparency (Art. 5 GDPR), insufficient information (Art. 13 / 14 GDPR) and lack of legal basis (Art. 6 GDPR). The obtained consents had not been given "specific" and not "unambiguous" (Art. 4 nr. 11 GDPR).
PORTUGAL	Portuguese Data Protection Authority (CNPD)	2018-07-17	400,000	Hospital	Art. 5 (1) (f) GDPR, Art. 32 GDPR	Investigation revealed that the hospital's staff, psychologists, dietitians and other professionals had access to patient data through their profiles. The profile management system appeared deficient - the hospital had 983 registered doctor profiles while only having 200 doctors. Moreover, doctors had unrestricted access to all patient files, regardless of the doctor's specialty.
POLAND	Polish National Personal Data Protection Office (UODO)	2019-09-28	219,530	Private company working with data from publicly available sources	Art. 14 GDPR	The fine concerned the proceedings related to the activity of a company which processed the data subject's data obtained from publicly available sources, enter aka from the Central Business Register and information on Economic Activity, and processed the data for commercial purposes. The authority verified non-compliance with the information

## POOBLAŠČENE OSEBE ZA VARSTVO PODATKOV



Upravljalcev in obdelovalcev imenujeta pooblaščen osebo za VOP, če:

- Obdelavo izvaja **javni organ**;
- predstavlja obdelava osebnih podatkov **temeljno dejavnost** oz. je zaradi narave dela potrebno **redno in sistematično spremljati** obelavo;
- se obdelujejo **posebne vrste osebnih podatki** (t.i. „občutljivi osebni podatki“).

Če gre za **povezano družbo** ali **organ z več enotam**, se lahko imenuje **ena oseba** za varstvo osebnih podatkov, ki zastopa (pod)družbe oz. enote organa.

Pooblaščen oseba za VOP je lahko zaposlena pri upravljalcu in obdelovalcu, lahko pa gre za **najeto zunanjo osebo**.

## OCENA UČINKA

Kadar je **verjetno**, da bi lahko **obdelava osebnih podatkov** predstavljala **veliko tveganje za pravice in svoboščine posameznikov**, upravljalcev pred obdelavo opravi **oceno učinka** predvidenih dejanj obdelave.

Ocena učinka se opravi predvsem, če:

- gre za **sistematično in obsežno obdelavo OP z avtomatiziranimi sredstvi**;
- gre za **obdelavo posebnih vrst osebnih podatkov**;
- gre za **obsežno sistematično spremljanje javno dostopnega območja**.



Če je iz **ocene učinka razvidno**, da bi obdelava osebnih podatkov predstavljala **veliko tveganje**, če ne bi bili sprejeti ukrepi za ublažitev tveganja, se upravljalcev **predhodno posvetuje z nadzornim organom**.

## URADNO OBVESTILO O KRŠITVI VARSTVA OP

### URADNO OBVESTILO INFORMACIJSKEMU POOBLAŠČENCU

V primeru kršitve varstva osebnih podatkov upravljalcev **brez nepotrebnega odlašanja, uradno obvesti pristojni nadzorni organ, razen če ni verjetno**, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov.

### OBVESTILO POSAMEZNIKU

Kadar je **verjetno**, da kršitev varstva osebnih podatkov povzroči **veliko tveganje za pravice in svoboščine posameznikov**, upravljalcev brez nepotrebnega odlašanja sporoči posamezniku, na katerega se nanašajo osebni podatki, da je **prišlo do kršitve** varstva osebnih podatkov.

#### Prednosti (samodejnega) sistema (samo)priljav:

- ✓ Odgovornost poročanja na strani upravljalcev in obdelovalcev.
- ✓ Nadzorni organ bo imel več informacij o kršitvah.
- ✓ Uredba skuša postopek poročanja o kršitvah standardizirati.

#### Slabosti (samodejnega sistema) (samo)priljav:

- ❖ Več dela za nadzorne organe, če bo (samo)priljav veliko.
- ❖ Praksa bo pokazala v kakšni meri in na kakšen način bo sistem poročanja zaživel.

## KAM NAPREJ?

INFORMACIJSKI POOBLAŠČENCI

REPUBLIKA SLOVENIJA

ZAKONODAJA | OBRAZCI | PUBLIKACIJE | O POOBLAŠČENCU

Varstvo osebnih podatkov za podjetja - različne oblike, vsebuje tudi na strani. [www.upravljalcev.si](http://www.upravljalcev.si)

Brezplačna telefonska podpora za podjetja

080 29 00

Varstvo osebnih podatkov

Novica

Članek do informacij z varstvom osebnih podatkov

[www.ip-rs.si](http://www.ip-rs.si)

[www.upravljalcev.si](http://www.upravljalcev.si)

[gp.ip@ip-rs.si](mailto:gp.ip@ip-rs.si)

[matjaz.drev@ip-rs.si](mailto:matjaz.drev@ip-rs.si)