



Javni štipendijski, razvojni,
invalidski in preživninski
sklad Republike Slovenije



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE,
ZNANOST IN ŠPORT



EVROPSKA UNIJA
EVROPSKI SKLAD
SOCIALNI SKLAD
NALOŽBA V VAŠO PRIHODNOST



Pravna fakulteta
Univerza v Ljubljani



Univerza v Ljubljani
Fakulteta
za računalništvo
in informatiko

Univerza v Ljubljani
Fakulteta za *matematiko in fiziko*



VOXIOR

PROJEKT V OKVIRU 4. RAZPISA JAVNEGA ŠTIPENDIJSKEGA, RAZVOJNEGA, INVALIDSKEGA IN
PREŽIVNINSKEGA SKLADARS »PO KREATIVNI POTI DO PRAKTIČNEGA ZNANJA 2017-2020«

VARSTVO ZASEBNOSTI IN PAMETNI DOMOVI

Tadej Baloh, Pravna fakulteta UL

Karin Dodič, Pravna fakulteta UL

Urban Marovt, Fakulteta za matematiko in fiziko UL

Matic Novak, Fakulteta za računalništvo in informatiko UL

Anja Šinkovec, Pravna fakulteta UL

Jana Šteblaj, Pravna fakulteta UL

Matic Tempfer, Fakulteta za računalništvo in informatiko UL

Aleksej Tomažič, Fakulteta za računalništvo in informatiko UL

v sodelovanju s podjetjem

Voxior d.o.o.

in mentorji

prof. dr. Marko Bajec, Fakulteta za računalništvo in informatiko UL, pedagoški mentor

prof. dr. Jerca Kramberger Škerl, Pravna fakulteta UL, pedagoška mentorica

Dejan Bukovnik, Voxior d.o.o., delovni mentor

Projekt sofinancirata Republika Slovenija in Evropska unija iz Evropskega socialnega sklada.

LJUBLJANA, JULIJ 2018

KAZALO VSEBINE

A. REZERVACIJE	4
B. SEZNAM OKRAJŠAV	5
C. SEZNAM PRILOG	6
D. POVZETEK	7
E. SUMMARY	9
F. UVOD	11
G. GLASOVNO UPRAVLJENJE PAMETNEGA DOMA	12
1. Splošno o pametnih domovih	12
2. Produkt podjetja Voxior	12
H. POTEK DELA PROJEKTA	14
I. SPLOŠNO O ZASEBNOSTI IN O VARSTVU OSEBNIH PODATKOV	15
J. SPLOŠNO O UREDBI GDPR	16
1. Sprememba pravne oblike akta	16
2. Obseg uporabe	16
2.1. Definicija osebnega podatka	16
2.2. Krajevna veljavnost	17
2.3. Osebna veljavnost	17
3. Osnovni pojmi	17
3.1. Osebni podatek	17
3.2. Obdelava	17
3.3. Upravljalavec in obdelovalec	18
K. PRAVNE PODLAGE ZA OBDELAVO OSEBNIH PODATKOV	19
1. Privolitev	19
1.1. Kdaj je potrebno pridobiti novo privolitev, ki je že bila pridobljena v skladu z Direktivo?	22
2. Pogodbeno razmerje	24
3. Izpolnitev zakonske obveznosti upravljavca	24
4. Življenjski interesi posameznika	25
5. Javni interes in izvrševanje javne oblasti	25
6. Zakoniti interesi, za katere si prizadeva upravljalavec ali tretja oseba	26
L. ANALIZA OBRAZCA ZA PRIDOBITEV SOGLASJA PODJETJA VOXIOR	27
1. Razdelitev po namenih obdelave	27
2. Obdobje hrambe	28
3. Avtomatizirano odločanje	28

4. Prenos osebnih podatkov v tretje države ali mednarodne organizacije.....	28
M. PRAVICE POSAMEZNIKOV	30
1. Pravica biti informiran.....	30
2. Pravica do dostopa.....	30
3. Pravica do popravka	30
4. Pravica do izbrisa	30
5. Pravica do omejitve obdelave.....	30
6. Pravica do prenosljivosti podatkov	31
7. Pravica do ugovora.....	31
8. Pravica, da niso podvrženi sprejemanju avtomatiziranih odločitev	31
N. OBVEZNOSTI UPRAVLJAVCEV IN OBDELOVALCEV	33
1. Izvajanje vgrajenega in privzetega varstva podatkov.....	33
2. Vodenje evidence dejavnosti obdelave	33
3. Obveznost obvestila o kršitvi	33
4. Narediti oceno učinkov	33
5. Imenovati pooblaščen osebe za varstvo podatkov.....	35
O. IZNOS PODATKOV V TRETJE DRŽAVE.....	37
1. Iznos osebnih podatkov v ZDA.....	39
P. DRUGE NOVOSTI.....	40
1. Poročaje v primeru varnostnega incidenta	40
2. Ureditev pogodbenih razmerij z obdelovalci podatkov	40
3. Pregled varnostnih politik in njihovega izvajanja	40
4. Praktični napotki zaposlenim	40
5. Zagrožene višine glob	41
Q. UGOTOVITVE IN SKLEP	43
R. LITERATURA IN VIRI.....	44
Članki.....	44
Pravni predpisi.....	44
Viri na medmrežju	44

POVZETEK

To študija z naslovom Varstvo zasebnosti in pametni domovi predstavlja skupek pomembnejših sprememb, ki so bile upoštevane pri uvedbi nove uredbe o varstvu osebnih podatkov, z uradnim nazivom: UREDBA (EU) 2016/679 EVROPSKEGA PARLAMENTA IN SVETA z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) v poslovanje družbe Voxior.

Splošna uredba o varstvu podatkov je stopila v veljavo dne 25.05.2018 in nadomešča nadomešča nacionalne ureditve, ki so se izvajale v državah članicah EU na podlagi sedanje Direktive 95/46 / ES (v nadaljnjem besedilu: »Direktiva«).

GDPR razširja definicijo osebnih podatkov in tako povečuje obseg pravnega varstva. V skladu z GDPR pomeni "osebni podatek" katero koli informacijo v zvezi z določenim ali določljivim posameznikom. Zaradi čezmejnega prenosa osebnih podatkov, GDPR razširja področje uporabe pravil o varstvu osebnih podatkov tudi zunaj EU, kolikor je dejavnost organizacije usmerjena na potrošnike v EU.

Obdelava osebnih podatkov je zakonita le, če in kolikor je podana vsaj ena od naslednjih pravnih podlag:

1. posameznik je privolil v obdelavo;
2. obdelava je potrebna za izvajanje pogodbe;
3. obdelava je potrebna za izpolnitev zakonske obveznosti (npr. za davčne razloge);
4. obdelava je potrebna za zaščito življenjskih interesov posameznika ali druge fizične osebe;
5. obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu;
6. obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba.

Najpogosteje uporabljena pravna podlaga za obdelavo podatkov je privolitev, ki pomeni vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi soglasje z obdelavo osebnih podatkov, ki se nanašajo nanj. Ključne posebnosti glede privolitve so: pridobiti jo je potrebno pred obdelavo osebnih podatkov; dokazno breme je na upravljavcu;

posameznik ima pravico, da dano privolitev kadarkoli umakne; potrebno je dati možnost ločenega soglasja za različne namene za obdelavo osebnih podatkov; da se privolitev šteje za informirano mora biti posameznik seznanjen vsaj z identiteto upravljavca in nameni obdelave, za katero so namenjeni osebni podatki; predznačena okenca ali neaktivnost ne pomeni privolitve.

Poleg pravic posameznikov, na katere se nanašajo osebni podatki, ki jih ureja že Direktiva, GDPR uvaja dve novi pravici, ki sta: »Pravica do izbrisa« (»pravica do pozabe«), ki pomeni, da ima posameznik, na katerega se nanašajo osebni podatki, pravico doseči, da upravljavec brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim; in »Pravica do prenosljivosti podatkov«, ki pomeni, da ima posameznik, na katerega se nanašajo osebni podatki, pravico, da prejme osebne podatke v zvezi z njim, ki jih je posedoval upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki, in pravico, da te podatke posreduje drugemu upravljavcu.

Poleg obveznosti upravljavcev in obdelovalcev gre poudariti še oceno učinkov varstva osebnih podatkov, saj predstavlja enega ključnih konceptov v okviru načela odgovornosti. Ta institut je namenjen pravočasnemu prepoznavanju tveganj in sprejemanju ustrezne ukrepov, da se prepreči kršitev zakonodaje. Ocene učinkov so potrebne v primerih kjer so tveganja glede varstva osebnih podatkov velika.

Poleg tega je ponovno uvedena obveznost imenovanja pooblaščenca za varstvo podatkov (»DPO«) za določene upravljavce in obdelovalce.

Nadalje GDPR za primere kršitve varstva osebnih podatkov uvaja višje globe in kazni.

Ključne besede:

GDPR, osebni podatki, posameznik na katerega se nanašajo osebni podatki, obdelovanje, privolitev, pravica do izbrisa, pravica do prenosljivosti podatkov, ocena učinkov varstva osebnih podatkov, pooblaščenec za varstvo podatkov

SUMMARY

The present »Protection of privacy and smart homes« report represents a set of major aspects of the changes that were taken into account in the introduction of the new REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter the »GDPR«) into the business of the company Voxior.

On 25 May 2018, the new General Data Protection Regulation became applicable, replacing the national arrangements implemented in the EU Member States on the basis of the current Directive 95/46/EC (hereinafter the »Directive«).

The GDPR extends the definition of personal data and thus increases the scope of legal protection. According to the GDPR, '*personal data*' means any information relating to an identified or identifiable natural person. Due to the cross-border transfer of personal data, the GDPR extends the scope of application of the rules on the protection of personal data also outside the EU, insofar as the activity of the organization is directed at consumers in the EU.

Processing of personal data is lawful only if and to the extent that at least one of the following legal basis is given:

7. the data subject has given consent to the processing
8. processing is necessary for the performance of a contract
9. processing is necessary for compliance with a legal obligation to which the controller is subject (*eg.* for taxation purposes);
10. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
11. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
12. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

The most commonly used basis for data processing is consent which means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The key specifics regarding of consent are: must be obtained before the processing of personal data; burden of proof is on the controller; data subject has the right

to withdraw the consent at any time; option of separate consent for various purposes for the processing of personal data must be given; for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended; pre-ticked boxes or inactivity do not constitute consent.

In addition to the rights of the data subjects, already determined in the Directive, the GDPR introduces two new rights, which are: the “Right to erasure” (‘right to be forgotten’), which means that the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay; and the “Right to data portability”, which means that the data subject shall have the right to receive the personal data concerning him or her, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller.

Among the obligations of controllers and processors, the data protection impact assessment must be emphasized, since it represents one of the key concepts within the framework of the principle of accountability. This institute is intended to timely identify risks and take appropriate measures, to prevent breach of legislation. Impact assessments are needed in cases where the risks regarding the protection of personal data are high. In addition, the obligation of designation of the data protection officer (»DPO«) for certain controllers and processors is again introduced.

Furthermore, the GDPR introduces higher fines and sanctions for cases of violation of the protection of personal data.

Keywords:

GDPR, personal data, data subjects, processing, consent, right to erasure, right to data portability, data protection impact assessment, data protection officer