

Poništava:	PK 04 v.1		
	Ime i prezime	Potpis	Datum
Prilagodio:	Silvija Češljaš, Službenik zaštite osobnih podataka		18.01.2021.
Odobrio:	Tomislav Kulić, Član Uprave		19.01.2021.
Odobrio:	Jasmin Huljaj, Predsjednik Uprave		

a PHOENIX company
Zagreb, Ozaljska 95

Povijest izmjena:

Verzija	Datum izmjene/revizije	Razlog promjene
1	25.05.2018.	Prva verzija dokumenta
2	01.02.2021.	Nova verzija Pravilnika o zaštiti osobnih podataka PHOENIX Grupe GGL_Corporate Data Protection_20210201.

Rječnik zaštite osobnih podataka društva

GSI	Glavni službenik za informacije
GSSI	Glavni službenik za sigurnost informacija
Vodič ZOPD	Vodič za zaštitu osobnih podataka društva
Koncept društva	Koncept zaštite osobnih podataka društva
Pravilnik o zaštiti osobnih podataka	Pravilnik o zaštiti osobnih podataka za cijelu PHOENIX Grupu
UOOP	Ugovor o obradi osobnih podataka
PUZOP (DPIA)	Procjena učinka na zaštitu osobnih podataka
SZOP	Službenik za zaštitu osobnih podataka
Zaposlenik	Osoba koja je zaposlena u PHOENIX Grupi.
EU/EGP	Europska unija / Europski gospodarski prostor
OUZP/GDPR	Opća uredba o zaštiti podataka (EU) 2016/679 (GDPR).
VZOPD	Voditelj zaštite osobnih podataka društva
LKS	Lokalni koordinator za sigurnost
Lokalni koncept	Koncept lokalne zaštite osobnih podataka
PUP	Procjena učinka na privatnost
Društvo PHOENIX	Podružnica koja pripada PHOENIX Grupi
PHOENIX Grupa	Obuhvaća sva društva u kojima većinu udjela drži PHOENIX Pharma SE ili jedno od njezinih društava-kćeri, ili koju izravno ili neizravno kontrolira holding društvo ili njegova društva-kćeri
NT	Nadzorno tijelo
SOP-ovi	Standardni operativni postupci
TOM-ovi	Tehničke i organizacijske mjere
Vlasnik obrade podataka	Direktor/voditelj odjela

Sadržaj

1.	Uvod.....	5
2.	Područje primjene	5
3.	Organizacija: uloge i odgovornosti u pogledu zaštite osobnih podataka	6
1.1	3.1 Izvršni odbor (razina Grupe)	6
1.2	3.2 Uprava (na razini Društva)	6
1.3	3.3 Zaposlenici	7
1.4	3.4 Vlasnik obrade podataka	7
1.5	3.5 Službenik za zaštitu osobnih podataka	8
1.6	3.6 Odjel za zaštitu osobnih podataka društva.....	9
1.7	3.7 Sigurnost informacija	9
4.	Pravni okvir za obradu osobnih podataka	10
1.8	Načelo 1: Zakonitost, poštenost i transparentnost	10
1.8.1		10
1.8.2	Posebna pravila za privolu	10
1.8.3		11
1.8.4	Posebna pravila o podacima posebne kategorije prema propisima o zaštiti osobnih podataka (OUZP) 11	
1.8.5	Zahtjevi za zaštitu podataka koji se odnose na zakonitost, poštenost i transparentnost.....	11
1.8.6	Zahtjevi za privolu.....	12
1.9		12
1.10	Načelo 2: Ograničavanje svrhe	12
1.10.1	Zahtjevi za zaštitu osobnih podataka koji se odnose na ograničenje svrhe.....	12
1.11		13
1.12	Načelo 3: Smanjenje količine podataka.....	13
1.12.1	Zahtjevi za zaštitu osobnih podataka koji se odnose na smanjenje količine podataka	13
1.13		13
1.14	Načelo 4: Točnost	13
1.14.1	Zahtjevi za zaštitu osobnih podataka koji se odnose na točnost	13
	Načelo 5: Ograničenje pohrane	13
1.14.2	Zahtjevi za zaštitu osobnih podataka koji se odnose na ograničenje pohrane	13
1.15		14
1.16	Načelo 6: Sigurnost (cjelovitost i povjerljivost)	14
1.16.1	Zahtjevi za zaštitu podataka koji se odnose na sigurnost (cjelovitost i povjerljivost)	14

1.17	Načelo 7: Odgovornost	15
1.17.1	Zahtjevi za zaštitu osobnih podataka koji se odnose na odgovornost	15
5.	Nova ili promijenjena aktivnost obrade osobnih podataka	15
1.18	5.1 Standardni pristup	15
1.19	5.2 Procjena učinka na zaštitu osobnih podataka (PUZOP).....	16
6.	Ugovori s pružateljima usluga.....	16
1.20	6.1 Pravila za angažiranje izvršitelja obrade.....	16
1.21	6.2 Pravila o prijenosu osobnih podataka izvan EU-a.....	17
1.22	6.3 Pravila za druge pružatelje usluga	17
7.	Ostvarivanje prava ispitanika.....	17
8.	Tehničke mjere za zaštitu osobnih podataka	18
9.	Izješćivanje o povredi osobnih podataka	18
1.23	9.1 Interno izješćivanje	18
1.24	9.2 Upravljanje povredom osobnih podataka	19
10.	Provedbene aktivnosti	19
1.25	10.1 Provedbene aktivnosti društva	19
1.26		20
1.27	10.2 Koncept zaštite osobnih podataka društva	20
1.28	10.3 Koncept lokalne zaštite osobnih podataka.....	21

1. Uvod

- (1) Živimo u svijetu koji se temelji na podacima. Naši kupci, zaposlenici ili poslovni partneri dijele svoje podatke s nama gotovo u svakoj transakciji i interakciji. Osobni su podaci informacije koje omogućuju izravnu ili neizravnu identifikaciju žive osobe iz podataka koji su dostupni, poput imena osobe, podataka o lokaciji, zdravstvenih podataka, ili mogu biti nešto manje očigledni, poput IP adresa.
- (2) Osobni podaci pripadaju živoj osobi (ispitanik). Odjel za zaštitu osobnih podataka osigurava da se svi osobni podaci koriste pravilno i zakonito. Pravni propisi o zaštiti osobnih podataka utvrđuju glavna načela i pravila za obradu osobnih podataka.
- (3) PHOENIX Grupa ozbiljno shvaća zaštitu osobnih podataka i privatnost svojih zaposlenika, poslovnih partnera i klijenata. Cilj je ovoga Pravilnika o zaštiti osobnih podataka osigurati da obrada osobnih podataka bude u skladu s pravnim propisom o zaštiti podataka i da odražava obveze i načela OUZP-a (GDPR-a).

2. PODRUČJE PRIMJENE

- (1) Ovaj se Pravilnik odnosi na obradu osobnih podataka i posebne kategorije osobnih podataka koje se odnose na žive osobe koje se mogu identificirati iz tih podataka. Primjenjuje se na osobne podatke koji su obrađeni elektronički ili koji su obrađeni na papiru i zatim pohranjeni u odgovarajućoj arhivi. U zemljama u kojima su osobni podaci pravnih osoba (npr. društva s ograničenom odgovornošću) zaštićeni u istoj mjeri kao i osobni podaci pojedinaca, ovaj se Pravilnik jednako odnosi na osobne podatke pravnih osoba.
- (2) Ovaj se Pravilnik odnosi na:
 - a) sve zaposlenike PHOENIX Grupe;
 - b) sva Društva PHOENIX;
 - c) subjekte s kojima je potpisan ugovor koji navodi da se ovaj Pravilnik mora provoditi kako bi se pristupilo podatkovnoj imovini grupe (partneri u zajedničkom pothvatu, franšizni partner itd.);
 - d) sve treće strane koje izravno pristupaju podatkovnoj imovini u vlasništvu ili pod izravnom kontrolom PHOENIX Grupe (npr. vanjski savjetnici);
 - e) svi pružatelji usluga koji izravno pristupaju podatkovnoj imovini u vlasništvu ili pod izravnom kontrolom PHOENIX Grupe. Oni moraju pokazati razinu usklađenosti s ovim Pravilnikom.
- (3) Bilo koji treći pružatelji usluga i ugovorni suradnici koji izravno pristupaju podatkovnoj imovini u vlasništvu ili pod izravnom kontrolom PHOENIX Grupe moraju se prema ugovoru uskladiti s ovim Pravilnikom i obvezati se na povjerljivost. Pružatelji usluga koji se smatraju izvršiteljem obrade osobnih podataka moraju potpisati ugovore o obradi osobnih podataka (vidi poglavlje 6).
- (4) Društvo PHOENIX primjenjuje svoje ovlasti u odnosu nad zaposlenicima i primjenjuje ovaj Pravilnik zajedno s lokalnim obvezujućim pravilima za zaposlenike, u skladu s lokalnim radnopravnim propisima.
- (5) Društvo PHOENIX osigurava da svi njegovi zaposlenici imaju prikladan pristup ovom Pravilniku na njihovu lokalnomu jeziku ako je potrebno, naročito putem intraneta. Mjerodavna je izvorna engleska inačica.

- (6) Ovaj je Pravilnik jedan od provedbenih aktivnosti neophodnih za postizanje usklađenosti s OUZP-om. Daljnje provedbene aktivnosti opisane su u poglavlju 10.
- (7) Nacionalni zakoni i propisi mogu biti stroži od OUZP-a i/ili ovoga Pravilnika. Sva Društva PHOENIX i njihovi zaposlenici moraju se pridržavati mjerodavnih lokalnih propisa.
- (8) Lokalna se prilagodba može napraviti, ali ne smije dovesti do toga da razina zaštite osobnih podataka padne ispod one opisane u ovom Pravilniku. Odstupanja od ovoga Pravilnika ili od standarda zaštite osobnih podataka društva može dopustiti samo iznimka PHOENIX Grupe (VZOPD, Izvršni odbor PHOENIX Grupe). Zahtjev i odobrenje za izuzeće moraju se dokumentirati. Predložak za zahtjev za izuzećem može se zatražiti od VZOPD-a.

3. ORGANIZACIJA: ULOGE I ODGOVORNOSTI U POGLEDU ZAŠTITE OSOBNIH PODATAKA

1.1 3.1 Izvršni odbor (razina Grupe)

- (1) Voditelj zaštite osobnih podataka društva (VZOPD) podržava Izvršni odbor PHOENIX Grupe pri organizaciji, provedbi, održavanju, provjeri i poboljšanju zaštite osobnih podataka društva. Izvršni odbor zahtijeva definirana izvješća od VZOPD-a.
- (2) Kako bi omogućio VZOPD-u obavljati njegove dužnosti, Izvršni odbor automatski obavještuje i, ako je primjenjivo, uključuje VZOPD-a na odgovarajući i pravodoban način o/u svim međunarodnim pitanjima, projektima, promjenama ili poslovima koji se odnose na obradu osobnih podataka (pasivno pravo na pristup informacijama). Izvršni odbor podržava VZOPD-a u obavljanju njegovih zadataka.
- (3) VZOPD ima na raspolaganju resurse koji odražavaju prirodu i složenost poslovnoga modela u grupi. VZOPD ima neovisno mjesto u organizaciji i podnosi izvještaje članu/članovima Izvršnoga odbora.

1.2 3.2 Uprava (na razini Društva)

- (1) Društvo PHOENIX provjerava je li imenovanje službenika za zaštitu osobnih podataka (SZOP) obvezatno prema lokalnim propisima i udovoljava li s tim povezanim pravnim zahtjevima (npr. obavijestiti nadzorno tijelo za zaštitu osobnih podataka, objaviti podatke za kontakt o lokalnomu SZOP-u itd.).
- (2) Ako ne postoji zakonska obveza imenovanja SZOP-a sukladno OUZP-u ili lokalnim propisima o zaštiti osobnih podataka, Društvo PHOENIX određuje kontakt-osobu za postupak zaštite osobnih podataka i komunikaciju s odjelom za zaštitu osobnih podataka društva. Za potrebe interne komunikacije, ta se osoba također interno zove SZOP. Ova skraćenica ne znači da je osoba službeno imenovana službenikom za zaštitu osobnih podataka u skladu s OUZP-om.
- (3) Svi treći pružatelji usluga koji djeluju kao SZOP Društva PHOENIX moraju po ugovoru biti u skladu s ovim Pravilnikom.
- (4) Društva PHOENIX iz jedne zemlje mogu odlučiti da ih jedna osoba predstavlja u komunikaciji s odjelom za zaštitu osobnih podataka društva.
- (5) SZOP – službeno ili interno imenovan – ima potrebne stručne kvalifikacije te znanje o pravilima i postupku zaštite osobnih podataka.
- (6) Kako bi omogućio SZOP-u obavljati njegove dužnosti, lokalna Uprava automatski obavještuje i, ako je primjenjivo, uključuje SZOP-a na odgovarajući i pravodoban način o/u svim

pitanjima, projektima, promjenama ili poslovima koji su povezani s propisima o zaštiti osobnih podataka. Lokalna Uprava podupire SZOP-a u obavljanju njegovih zadataka.

- (7) SZOP ima na raspolaganju resurse koji odražavaju prirodu i složenost poslovnoga modela u Društvu PHOENIX. SZOP ima neovisno mjesto u Društvu PHOENIX i podnosi izvještaje najvišoj razini upravljanja.
- (8) Uprava, bez obzira obavlja li ili ne ulogu obrade, odgovorna je za zaštitu osobnih podataka. Uprava osigurava usklađenost s propisima o zaštiti osobnih podataka i ovim Pravilnikom, npr. uspostavljanjem primjerenih organizacijskih jedinica i postupaka tako da operativno upravljanje ima na raspolaganju sredstva i ovlasti za obavljanje uloge vlasnika obrade i učinkovito osiguravanje usklađenosti.
- (9) Svi zaposlenici moraju imati odgovarajući pristup postojećim pravilnicima i postupcima o zaštiti osobnih podataka koji odgovaraju radnomu mjestu. Pravilnici, postupci te odgovornosti i funkcije u vezi sa zaštitom osobnih podataka redovito se prate i ažuriraju (svake 2 godine); službenik za zaštitu osobnih podataka odgovoran je za ovo lokalno praćenje.

1.3 3.3 Zaposlenici

- (1) Od svih zaposlenika očekuje se da čuvaju povjerljivost osobnih podataka koje obrađuje Društvo PHOENIX. Ova se obveza unosi u ugovor o radu i/ili u dokumente za zapošljavanje.
- (2) Odgovarajuća obuka o zaštiti osobnih podataka (na mreži i/ili osobno) obvezatna je za svakoga zaposlenika u PHOENIX Grupi uzimajući u obzir radno mjesto i odgovornost. Plan obuke pripada provedbenim aktivnostima (vidi poglavlje 10).
- (3) Svi zaposlenici podržavaju SZOP-a i VZOPD-a u obavljanju njihovih dužnosti, npr. davanjem pristupa osobnim podacima (u slučaju ispitanikova zahtjeva) i postupcima obrade na zahtjev, pružanjem informacija ili predajom dokumenata.
- (4) Svi zaposlenici uključuju SZOP-a/VZOPD-a u ranim koracima u sva pitanja koja se odnose na zaštitu osobnih podataka.
- (5) Svi zaposlenici poštuju i pridržavaju se načela zaštite osobnih podataka prilikom obrade osobnih podataka (vidi poglavlje 4).
- (6) Svi zaposlenici interno prijavljuju povredu osobnih podataka (vidi poglavlje 9).

1.4 3.4 Vlasnik obrade podataka

- (1) Zaposlenik u Društvu PHOENIX koji je organizacijski odgovoran za poslovni postupak ili interni postupak u kojemu se obrađuju osobni podaci smatra se vlasnikom obrade podataka.
- (2) Vlasnik obrade podataka odgovoran je za tzv. aktivnost obrade. Aktivnost obrade jest skup poslova, poput određene poslovne obrade ili IT alata.
- (3) Vlasnik obrade podataka imenovan je u izvještajima o aktivnostima obrade imenom ili funkcijom (vidi poglavlje 5).
- (4) Pri planiranju, uvođenju i kasnijoj promjeni aktivnosti obrade, Vlasnik obrade mora se pridržavati sljedećih pravila:
 - a) Uključiti SZOP-a u vezi s (pret)procjenom učinka na privatnost;
 - b) Napraviti procjenu učinka na zaštitu osobnih podataka, ako je obvezatna (vidi poglavlje 5);

- c) Dopuniti i održavati evidenciju o aktivnostima obrade (vidi poglavlje 5);
 - d) Osigurati informacije za ispitanike o obradi osobnih podataka;
 - e) Osigurati poštovanje načela zaštite osobnih podataka tijekom obrade (uključivanjem nadležnih odjela);
 - f) Provjeriti vanjskoga pružatelja usluga; ako pružatelji usluga obrađuju osobne podatke za Društvo PHOENIX u ime i u skladu s uputama društva, osigurati sklapanje ugovora o obradi osobnih podataka;
 - g) Osigurati da se prava ispitanika mogu ispuniti;
 - h) Osigurati da su prava pristupa i razdoblja pohrane određeni provedbom.
 - i) Pri prijenosu osobnih podataka u zemlje koje nisu EU-u/EGP-u, uključiti SZOP-a i poštovati posebne zahtjeve za obradu osobnih podataka izvan EU-a/EGP-a;
 - j) Sve dokumentirati tako da se može dokazati usklađenost s propisima o zaštiti osobnih podataka.
- (5) Tehničko održavanje aktivnosti obrade može se prenijeti vanjskomu pružatelju (vidi poglavlje 6) ili odjelu IT-a, ali vlasnik obrade podataka i dalje je odgovoran za ispunjavanje gore navedenih pravila. SZOP pomaže vlasniku obrade i savjetuje ga.
- (6) Društvo PHOENIX može definirati vlastitu odgovarajuću organizaciju za upravljanje zaštitom osobnih podataka i shodno tomu njezinu terminologiju, uloge i odgovornosti. Ulogu vlasnika obrade podataka pokriva definirana organizacija.

1.5 3.5 Službenik za zaštitu osobnih podataka

- (1) Glavni je zadatak SZOP-a zaštita privatnosti ispitanika u vezi s obradom osobnih podataka na razini društva/države (podaci kupaca, pacijenata, zaposlenika itd.). SZOP je službena kontakt-točka za ispitanike i za nadzorno tijelo.
- (2) SZOP je odgovoran za savjetovanje organizacije i zaposlenika u vezi sa zaštitom osobnih podataka. SZOP je odgovoran za praćenje usklađenosti s propisima o zaštiti osobnih podataka. SZOP definira sadržaj lokalnoga koncepta (pojedini pogledajte u poglavlju 10).
- (3) Glavne su odgovornosti SZOP-a sljedeće:
- Podizanje svijesti: kampanje i programi obuke;
 - Održavanje lokalnoga pravilnika o zaštiti osobnih podataka i srodnih pravilnika ili uputa;
 - Održavanje predložaka zemalja (ugovor o obradi osobnih podataka, obavijest o privatnosti, privola itd.);
 - Podrška u pregovaranju o ugovoru o obradi osobnih podataka (UOOP): provjera glavnih ugovora o obradi osobnih podataka i tipskih klauzula EU-a; SZOP kao podrška pravnomu odjelu / odjelu nabave;
 - Početna procjena novih lokalnih projekata: definicija zahtjeva i preporuka za zaštitu osobnih podataka;
 - Pomoć u provođenju procjena učinka na zaštitu osobnih podataka;
 - Pomoć u stvaranju i održavanju evidencije o aktivnostima obrade;
 - Koordinacija ostvarivanja prava ispitanika: održavanje internih postupaka pri ostvarivanju prava ispitanika;

- Podrška pri upravljanju incidentima s osobnim podacima i upravljanje slučajevima povrede osobnih podataka: koordinacija i pomoć u izvješćivanju nadzornom tijelu / ispitaniku;
 - Upravljanje i savjetovanje: stalno praćenje usklađenosti zaštite osobnih podataka.
- (4) SZOP obavještava VZOPD-a o pitanjima o zaštiti osobnih podataka ili velikim projektima u vezi sa zaštitom osobnih podataka u Društvu PHOENIX. SZOP svake godine ili na zahtjev izvješćuje VZOPD-a tzv. izvješćima po zemljama.

1.6 3.6 Odjel za zaštitu osobnih podataka društva

- (1) Glavni je zadatak odjela za zaštitu osobnih podataka društva podržati PHOENIX Grupu i SZOP-ove u postupcima zaštite osobnih podataka.
- (2) VZOPD ima slične zadaće kao SZOP, ali u međunarodnom kontekstu. VZOPD savjetuje i prati usklađenost propisa o zaštiti osobnih podataka u grupi; VZOPD koordinira i podržava međunarodnu suradnju na području zaštite osobnih podataka.
- (3) VZOPD definira sadržaj koncepta društva (detalje vidi u poglavlju 10).
- (4) Glavne su odgovornosti VZOPD-a sljedeće:
 - Podizanje svijesti: kampanje i programi obuke (uključujući mrežnu obuku PHOENIX Grupe).
 - Održavanje Pravilnika o zaštiti osobnih podataka za cijelu grupu.
 - Izrada standarda zaštite osobnih podataka društva.
 - Podrška u pregovorima o međunarodnom ugovoru o obradi osobnih podataka (UOOP).
 - Početna procjena novih lokalnih/međunarodnih projekata: definicija zahtjeva i preporuka za zaštitu osobnih podataka.
 - Pomoć u provođenju procjena učinka na zaštitu osobnih podataka na razini grupe (predlošci društva za lokalne SZOP-ove).
 - Održavanje sustava izvješćivanja o povredi osobnih podataka grupe: administrator za platformu za izvješćivanje.
 - Održavanje upravljanja povredama osobnih podataka: koordinacija i pomoć u izvješćivanju nadzornom tijelu / ispitaniku, u slučajevima međunarodne prirode.
 - Savjetovanje i stalno praćenje usklađenosti zaštite osobnih podataka.
- (5) Član(ovi) odjela za zaštitu osobnih podataka društva podržava(ju) VZOPD-a svojim aktivnostima u određenim područjima u lokalnom ili međunarodnom području. Član tima u odjelu za zaštitu osobnih podataka društva vezan je uputama VZOPD-a i podnosi izvješća izravno VZOPD-u.

1.7 3.7 Sigurnost informacija

- (1) Glavni službenik za sigurnost informacija (GSSI) dužan je osigurati i primijeniti standarde sigurnosti informacija u PHOENIX Grupi. Zbog toga GSSI uspostavlja odgovarajuće pravilnike, smjernice i standarde za sigurnost te definira sadržaj sigurnosnoga koncepta za PHOENIX Grupu.

- (2) GSSI i lokalni koordinator za sigurnost (LKS) odgovorni su za provedbu i dokumentaciju tehničkih i organizacijskih mjera (TOM) radi zaštite osobnih podataka. Dokumentacija TOM-ova služi za dokazivanje usklađenosti s načelom sigurnosti OUZP-a (vidi poglavlje 4).
- (3) Suradnja i komunikacija između GSSI-a i VZOPD-a te LKS-a i SZOP-a na lokalnoj razini s obzirom na TOM-ove bliske su. VZOPD/SZOP navodi glavne zahtjeve za TOM-ove.
- (4) LKS podržava SZOP-a tijekom provjere pružatelja usluga. LKS provjerava TOM-ove pružatelja usluga koji se smatraju izvršiteljem obrade osobnih podataka (vidi poglavlje 6).

4. PRAVNI OKVIR ZA OBRADU OSOBNIH PODATAKA

- (1) Popis u nastavku daje pregled općepriznatih načela zaštite osobnih podataka prema modelu iz članka 5. OUZP-a.
- (2) Svi zaposlenici moraju poštovati i pridržavati se načela zaštite osobnih podataka prilikom obrade osobnih podataka. Svi zaposlenici slijede zahtjeve za zaštitu osobnih podataka sukladno svojoj funkciji i ulozi u PHOENIX Grupi i/ili u Društvu PHOENIX.

1.8 Načelo 1: Zakonitost, poštenost i transparentnost

- (1) Obrada osobnih podataka mora biti poštena; tj. ne poduzima se neočekivana ili obmanjujuća obrada osobnih podataka. Ispitanika se mora obavijestiti o važnim pojedinostima o obradi njegovih osobnih podataka.
- (2) Osobni podaci mogu se obrađivati samo ako postoji pravna osnova za obradu osobnih podataka. Postoji šest raspoloživih pravnih osnova za obradu osobnih podataka:
 - (a) **Privola:** pojedinac je dao jasan pristanak za obradu svojih osobnih podataka u određenu svrhu.
 - (b) **Ugovor:** obrada je potrebna za ugovor koji je Društvo PHOENIX sklopilo s pojedincem ili zato što postoje posebni koraci prije sklapanja ugovora.
 - (c) **Pravna obveza:** obrada je neophodna u skladu s propisom (ne uključujući ugovorne obveze).
 - (d) **Životno važni interesi:** obrada je neophodna za zaštitu nečijega života.
 - (e) **Javni zadatak:** obrada je potrebna za obavljanje zadatka u javnomu interesu ili za službenu funkciju, a zadatak ili funkcija ima jasnu zakonsku osnovu.
 - (f) **Legitimni interesi:** obrada je potrebna radi legitimnih interesa Društva PHOENIX ili legitimnih interesa treće strane, osim ako postoji opravdana svrha za zaštitu osobnih podataka pojedinca, koja prevladava nad tim legitimnim interesima.
- (3) Ako bi se ista svrha mogla postići bez obrade osobnih podataka, ne daje se pravna osnova. Pravnu osnovu mora se definirati prije početka obrade i mora ju se dokumentirati u evidenciji o aktivnostima obrade (vidi poglavlje 5).
- (4) Nijedna osnova nije važnija od ostalih – koja će osnova biti najprikladnija, ovisit će o svrsi/svrhama i odnosu s ispitanikom.

1.8.1

1.8.2 Posebna pravila za privolu

- (1) Privola nije sama po sebi bolja ili važnija od gore navedenih alternativa. Privola znači nuđenje stvarnoga izbora i kontrole pojedincima.

- (2) Privola se mora dati dobrovoljno. Privola bi trebala biti jasna i zahtijevati pozitivan odgovor za davanje privole. Ne postoji vremensko ograničenje za privolu, a trajanje privole ovisi o kontekstu obrade osobnih podataka.

1.8.3

1.8.4 Posebna pravila o podacima posebne kategorije prema propisima o zaštiti osobnih podataka (OUZP)

- (1) OUZP definira podatke posebne kategorije kao što su:
- osobni podaci koji otkrivaju rasno ili etničko podrijetlo;
 - osobni podaci koji otkrivaju politička mišljenja;
 - osobni podaci koji otkrivaju vjerska ili filozofska uvjerenja;
 - osobni podaci koji otkrivaju članstvo u sindikatu;
 - genetski podaci;
 - biometrijski podaci (ako se koriste radi identifikacije);
 - podaci koji se odnose na zdravlje;
 - podaci o spolnomu životu osobe;
 - podaci koji se odnose na spolno opredjeljenje osobe.
- (2) Za obradu posebnih kategorija osobnih podataka vrijede stroža pravila. Uz pravnu osnovu mora se zadovoljiti jedan od posebnih uvjeta u članku 9. OUZP-a:
- (a) izričita privola
 - (b) zapošljavanje, socijalna sigurnost i socijalna zaštita (ako je zakonom odobreno)
 - (c) životno važni interesi
 - (d) neprofitna tijela
 - (e) podaci koje je objavio ispitanik
 - (f) pravni zahtjevi ili sudski akti
 - (g) razlozi od značajna javnoga interesa (s pravnom osnovom)
 - (h) zdravstvena ili socijalna skrb (s pravnom osnovom)
 - (i) javno zdravlje (s pravnom osnovom)
 - (j) arhiviranje, istraživanje i statistika (s pravnom osnovom)
- (3) SZOP mora biti uključen u svako planiranje ili projekte koji se odnose na obradu posebne kategorije osobnih podataka.

1.8.5 Zahtjevi za zaštitu podataka koji se odnose na zakonitost, poštenost i transparentnost

- Utvrditi jasnu pravnu osnovu prije početka obrade.
- Paziti da aktivnost obrade ne prelazi ograničenja ove pravne osnove.
- Savjetovati se oko prave osnove sa SZOP-om i dokumentirati ju u skladu s lokalnim pravilima.
- Uključiti SZOP-a ako se radi o podacima posebne kategorije.
- Osigurati da su obrade, svrhe i pravna osnova u potpunosti dokumentirani.
- Obavijestiti ispitanike o obradi, npr. njezinoj svrsi i identitetu voditelja obrade u obavijesti o privatnosti; jasno komunicirati s ispitanicima o tomu kako, u kojoj mjeri i u koje će se svrhe obrađivati njihovi osobni podaci.
- Poštovati prava pojedinaca na pristup i ispravak njihovih podataka.

- Razvijati postupke i upute koji jasno objašnjavaju kako ispitanici mogu ostvariti svoja prava na pristup i ispraviti svoje podatke u svakom koraku obrade osobnih podataka.
- Primijeniti funkcije u sustavu kako bi se odgovorilo na zahtjeve za pristup, izmjenu ili blokiranje te na prigovore o obradi.
- Usvojiti interna pravila radi provjere valjanosti pravne osnove u slučaju promjene, npr. povlačenja privole.

1.8.6 Zahtjevi za privolu

- Privola mora izričito sadržavati ime voditelja obrade (Društvo PHOENIX), svrhe obrade i vrste aktivnosti obrade.
- Izričita privola mora biti izričito potvrđena riječima, a ne bilo kojim drugim pozitivnim odgovorom; nejasna ili opća privola nije dovoljna.
- Privola zahtijeva pozitivan odgovor. Ne koristiti unaprijed označena polja ili bilo koji drugi način zadane privole.
- Zahtjeve za privolu držati odvojeno od ostalih uvjeta (zahtjevi za privolu moraju biti istaknuti, odvojeni od ostalih uvjeta, sažeti te lako razumljivi i jednostavni za ispunjavanje).
- Izbjegavati zahtijevati privolu za obradu kao preduvjet određene usluge.
- Olakšati ljudima povući njihovu privolu i objasniti im kako to učiniti.
- Pohranjivati dokaze o privoli – tko, kad, kako i što je priopćeno ljudima.

1.9

1.10 Načelo 2: Ograničavanje svrhe

- (1) Osobni podaci prikupljaju se u određene, izričite i legitimne svrhe te se ne obrađuju dalje na način koji nije u skladu s tim svrhama.
- (2) Ako je nova svrha kompatibilna, nova pravna osnova nije potrebna za daljnju obradu.
- (3) Ako se nova svrha ili znatno razlikuje od izvorne, ili bi bila neočekivana, ili bi imala neopravdan utjecaj na pojedinca, vjerojatno je nespojiva s vašom izvornom svrhom.

1.10.1 Zahtjevi za zaštitu osobnih podataka koji se odnose na ograničenje svrhe

- Obradivati osobne podatke samo u određene izričite, legitimne i ograničene svrhe;
- Ograničiti obradu osobnih podataka putem informatičkoga sustava na prvenstveno određenu svrhu.
- Osigurati ograničenje svrhe ako se različite vrste osobnih podataka prikupljaju i obrađuju u različite svrhe.
- Usvojiti interna pravila za procjenu potreba usklađenosti od slučaja do slučaja kako bi se omogućila promjena svrhe.
- Naveći svrhu ili svrhe obrade osobnih podataka unutar dokumentacije koju je potrebno voditi kao dio evidencije o obradi (dokumentaciji) obveza prema članku 30. OUZP-a.
- Jasno komunicirati s ispitanicima o bilo kojoj promjeni primarno određene svrhe obrade njihovih osobnih podataka.

1.11

1.12 Načelo 3: Smanjenje količine podataka

- (1) Osobni podaci moraju biti primjereni, relevantni i ograničeni na ono što je potrebno u odnosu na svrhe u koje se obrađuju.
- (2) Osobni se podaci brišu ako više nisu potrebni.

1.12.1 Zahtjevi za zaštitu osobnih podataka koji se odnose na smanjenje količine podataka

- Utvrditi najmanju količinu osobnih podataka potrebnu za ispunjenje svrhe; sačuvati toliko informacija, ali ne i više od toga.
- Redovito provjeravati jesu li osobni podaci i dalje bitni i prikladni za te svrhe pa izbrišite sve što više nije potrebno.
- Razmotriti i upotrijebiti, ako je to moguće, posebne tehnologije za poboljšanje privatnosti koje omogućuju izbjegavanje pretjerane upotrebe osobnih podataka ili omogućivanje upotrebe anonimnih podataka.
- Osigurati da su osobni podaci primjereni, relevantni i ne prekomjerni za tu svrhu.

1.13

1.14 Načelo 4: Točnost

- (1) Osobni podaci moraju biti točni i, prema potrebi, ažurirani.
- (2) Treba poduzeti sve razumne korake kako bi se osiguralo da se osobni podaci, za koje se utvrdi da su netočni i uzimajući u obzir svrhe u koje se obrađuju, odmah izbrišu ili isprave.

1.14.1 Zahtjevi za zaštitu osobnih podataka koji se odnose na točnost

- Osigurati da su osobni podaci točni i ažurirani.
- Provesti postupke kako bi se osigurala i održala točnost obrađenih podataka, npr. automatskom provjerom kvalitete informacija unesenih u sustav prije obrade.
- Osigurati da ispitanik može ispraviti podatke koji više nisu točni.

Načelo 5: Ograničenje pohrane

- (1) Osobni podaci ne smiju se čuvati u obliku koji dozvoljava identifikaciju ispitanika dulje nego što je nužno za svrhe u koje se ti osobni podaci obrađuju.
- (2) Vlasnik obrade podataka određuje razdoblje zadržavanja/brisanja i unosi ga u pravilnik o zadržavanju Društva PHOENIX.
- (3) Svako Društvo PHOENIX održava pravilnik o zadržavanju/brisanju

1.14.2 Zahtjevi za zaštitu osobnih podataka koji se odnose na ograničenje pohrane

- Osobne podatke čuvati onoliko dugo koliko je potrebno za izvorno navedenu svrhu.
- Unaprijed odrediti vrijeme zadržavanja podataka koji se čuvaju u obliku koji omogućuje identifikaciju ispitanika.
- Osigurati da su potrebna razdoblja zadržavanja proporcionalna svrhama prikupljanja osobnih podataka i da su vremenski ograničena.

- Dodijeliti i odvojeno upravljati vremenom zadržavanja vezanim uz osobne podatke prikupljene u različite svrhe.
- Poseban oprez mora se poduzeti ako se osobni podaci pohranjuju na papiru jer je njihovu postojanju teško ući u trag.
- Značajke sustava osmišljenoga za upravljanje vremenom zadržavanja i izvođenje potrebnih naknadnih radnja: brisanje ili anonimizacija.

1.15

1.16 Načelo 6: Sigurnost (cjelovitost i povjerljivost)

- (1) Društvo PHOENIX poduzima odgovarajuće tehničke i organizacijske mjere (TOM) za zaštitu osobnih podataka na način koji je proporcionalan povezanim rizicima privatnosti.

Rizik za privatnost ispitanika može proizaći naočito iz:

- neplanirana uništavanja osobnih podataka i/ili
- gubitka osobnih podataka i/ili
- neplanirane izmjene osobnih podataka i/ili
- neovlaštena otkrivanja osobnih podataka i/ili
- neovlaštena pristupa osobnim podacima.

- (2) Sljedeće procjene odgovarajućih TOM-ova uzimaju se u obzir:

- najnovija dostignuća i
- troškovi provedbe i
- priroda, opseg, kontekst i svrhe obrade te
- rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode ispitanika (tj. rizik za privatnost kupaca ili zaposlenike itd.).

- (3) TOM-ovi moraju osigurati 'povjerljivost, cjelovitost i dostupnost' PHOENIXOVIH sustava i usluga te osobnih podataka koji se u njima obrađuju.

1.16.1 Zahtjevi za zaštitu podataka koji se odnose na sigurnost (cjelovitost i povjerljivost)

- Slijediti pravilnike o sigurnosti informacija, smjernice, standarde ili materijale za podizanje svijesti.
- Uključiti LKS-ove ili GSSI-ove u aktivnosti obrade ako je to obvezatno prema grupnomu ili lokalnomu pravilniku.
- Razmotriti stvari poput procjene rizika, organizacijskih pravilnika ili tehničkih mjera pri planiranju aktivnosti obrade.
- Na temelju procjene rizika osmisliti i primijeniti organizacijske i tehničke mjere za ublažavanje rizika na prihvatljivu razinu.
- Izbjegavati aktivnosti obrade za koje ublažavanje ne bi bilo učinkovito.
- Osigurati da odgovorno rukovodstvo donese jasnu odluku o tomu koji su rizici prihvaćeni i zašto.
- Ako je prikladno, upotrijebiti mjere poput pseudonimizacije i enkripcije.

Zahtjevi koji se odnose na sigurnost informacija

Povjerljivost:

Osobni podaci moraju biti zaštićeni od neovlaštena ili nenamjerna otkrivanja. Moraju se uzeti u obzir i vanjski i unutarnji napadači (npr. hakeri, frustrirani ili znatiželjni zaposlenici), kao i nemarne ili organizacijske prijetnje (npr. neobučeni zaposlenici, koncept dodijeljenih ovlaštenja).

Cjelovitost:

Osobni podaci moraju se dati u potpunosti i ispravno. Neovlaštene promjene osobnih podataka moraju se identificirati (npr. putem dnevnika/zapisnika) i moraju se osigurati postupci za ispravak.

Dostupnost:

Osobni podaci moraju biti dostupni po potrebi. Ovo također zahtijeva da se mogu obnoviti u slučaju gubitka ili uništenja (npr. sigurnosne kopije).

Mora postojati postupak redovite provjere, procjene i vrjednovanja učinkovitosti TOM-ova (npr. test prodornosti, vanjska i unutarnja provjera).

1.17 Načelo 7: Odgovornost

- (1) Društvo PHOENIX dužno je osigurati da može pokazati usklađenost s gore navedenim načelima OUZP-a.
- (2) Dokazi su ključan zadatak svih bitnih zaposlenika. Kad se održavaju mehanizmi odgovornosti, izrađuje se dokumentacija. Ta se dokumentacija može koristiti kao dokaz odgovornosti, vlasništva i usklađenosti s OUZP-om.
- (3) Društvo PHOENIX mora voditi potpunu evidenciju o aktivnostima obrade. Svi zaposlenici, naročito vlasnici procesa, dužni su unaprijed obavijestiti SZOP-a (prije donošenja planova) o novim ili promijenjenim aktivnostima obrade (vidi poglavlje 5).

1.17.1 Zahtjevi za zaštitu osobnih podataka koji se odnose na odgovornost

- Pobrinuti se da se usklađenost s gore navedenim načelima može dokazati u odgovarajućoj dokumentaciji.
- Obavijestiti SZOP-a o novoj ili promijenjenoj aktivnosti obrade unaprijed, ostavljajući mu dovoljno vremena za procjenu aktivnosti obrade.

5. NOVA ILI PROMIENJENA AKTIVNOST OBRADE OSOBNIH PODATAKA

1.18 5.1 Standardni pristup

- (1) SZOP mora unaprijed biti uključen u svaku novu aktivnost obrade. Vlasnik procesa ili voditelj projekta odgovoran je za primjereno savjetovanje sa SZOP-om.
- (2) SZOP provjerava pravnu osnovu za obradu osobnih podataka. SZOP navodi glavne zahtjeve za zaštitu osobnih podataka pri procjeni učinka na privatnost (PUP). Opseg PUP-a ovisi o aktivnosti obrade. SZOP savjetuje ako je procjena učinka na zaštitu osobnih podataka (PUZOP) obvezatna (vidi točku 5.2).

- (3) Ako je aktivnost obrade ili projekt međunarodnoga karaktera, također treba uključiti i VZOPD-a. VZOPD izvodi PUP/PUZOP Društva kao predložak za lokalni PUP/PUZOP; lokalni SZOP mora na lokalnoj razini provjeriti lokalne zahtjeve zaštite osobnih podataka. VZOPD također provjerava pružatelje usluga i/ili priprema drugu dokumentaciju/predloške (npr. obavijest o privatnosti). VZOPD unaprijed obavještava SZOP-a o svakoj međunarodnoj obradi osobnih podataka.
- (4) Ishod PUP-a pruža odgovarajuće pojedinosti za evidenciju o aktivnostima obrade. Obvezatni sadržaj evidencije utvrđen je člankom 30. OUZP-a. Za ispunjavanje evidencije odgovoran je vlasnik obrade. Za postupak vođenja evidencije o aktivnosti obrade odgovoran je SZOP.

1.19 5.2 Procjena učinka na zaštitu osobnih podataka (PUZOP)

- (1) Vlasnik obrade podataka odgovoran je za obavljanje PUZOP-a. PUZOP mora uključiti SZOP-a i LKS-a (i/ili VZOPD-a/GSSI-a za međunarodne projekte) te daljnje dionike (npr. radni savjetnici, IT arhitekti, pravni odjel itd.).
- (2) PUZOP je postupak za identifikaciju i smanjenje rizika za zaštitu podataka od aktivnosti obrade; tj. projekta. PUZOP je obavezan prema OUZP-u za obradu koja će vjerojatno dovesti do visoka rizika za pojedince. Ovo uključuje neke određene vrste obrade, ali je također dobra praksa napraviti PUZOP za bilo koji drugi veći projekt koji zahtijeva obradu osobnih podataka. PUZOP je potreban u sljedećim situacijama:
 - uvođenje novih tehnologija,
 - automatizirana obrada, uključujući profiliranje, koja dovodi do donošenja odluka koje proizvode pravne učinke na pojedince,
 - obrada podataka velikih razmjera posebne kategorije,
 - obrada kriminalnih radnja,
 - sustavno praćenje javno dostupna područja u velikim razmjerima itd.
- (3) PUZOP mora:
 - opisati prirodu, opseg, kontekst i svrhe obrade; i
 - procijeniti nužnost, proporcionalnost i mjere usklađenosti; i
 - prepoznati i procijeniti rizike za pojedince; i
 - utvrditi sve dodatne mjere za ublažavanje tih rizika.

Kako bi procijenio razinu rizika, Društvo PHOENIX mora uzeti u obzir vjerojatnost i ozbiljnost bilo kakva učinka na pojedince. Visok rizik može proizaći ili iz velike vjerojatnosti neke štete ili iz manje mogućnosti ozbiljne štete.

- (4) U okolnostima u kojima PUZOP ukazuje na to da bi obrada dovela do visoka rizika za prava i slobode ispitanika u slučaju da voditelj obrade ne poduzme mjere za ublažavanje rizika, SZOP se savjetuje s lokalnim nadzornim tijelom.

6. UGOVORI S PRUŽATELJIMA USLUGA

1.20 6.1 Pravila za angažiranje izvršitelja obrade

- (1) Pružatelj usluga smatra se izvršiteljem obrade ako pružatelj djeluje u ime i samo prema uputama Društva PHOENIX.

- (2) Ako Društvo PHOENIX odluči koristiti usluge izvršitelja obrade povezane s obradom podataka, mora se sklopiti ugovor o obradi osobnih podataka (UOOP). Za obradu osobnih podataka unutar grupe primjenjuje se poseban predložak i postupak za UOOP.
- (3) Ako UOOP izvršitelja obrade odstupa od UOOP-a lokalnoga ili predloška društva, konačnu inačicu mora odobriti SZOP ili pravni odjel. Provjeru treba pokrenuti vlasnik obrade podataka.
- (4) Sastavni dio pregovora o UOOP-u jest provjera TOM-ova pružatelja usluga / izvršitelja obrade. Tijekom te provjere moraju se provjeriti TOM-ovi pružatelja usluga kako bi se osiguralo da su u skladu s OUZP-om, naročito s obzirom na sigurnost osobnih podataka (čl. 32. OUZP-a). Ovu provjeru koordinira SZOP uz podršku LKS-a.
- (5) UOOP se mora sklopiti u pisanu obliku i mora se dokumentirati.
- (6) Redovito se obavlja revizija pružatelja usluga koji se smatraju izvršiteljima obrade. Plan revizije zaštite osobnih podataka za pružatelja usluga (uključujući razdoblje za reviziju) uzima u obzir rizik za privatnost koji se odnosi na aktivnosti obrade. Najkraće je razdoblje za reviziju 24 mjeseca. SZOP i LKS podržavaju vlasnika procesa pri reviziji. Plan revizije zaštite osobnih podataka spada u provedbene aktivnosti (vidi poglavlje 10).

1.21 6.2 Pravila o prijenosu osobnih podataka izvan EU-a

- (1) OUZP ograničava prijenose osobnih podataka izvan EU-a/EGP-a, osim ako su prava ispitanika zaštićena na drugi način ili ako se primjenjuje jedna od ograničena broja iznimaka u OUZP-u.
- (2) Društvo PHOENIX uvijek mora poznavati cijeli lanac opskrbe (koje društvo / koja država / koja usluga / koja kategorija osobnih podataka). Društvo PHOENIX mora jamčiti razinu zaštite osobnih podataka OUZP-a u cijelomu lancu obrade.
- (3) Prikladna razina zaštite u zemlji/pružatelju usluga izvan EU-a/EGP-a osigurava se određenim jamstvima koja su unaprijed određena u OUZP-u (npr.):
 - odluka Komisije o primjerenosti
 - obvezujuća pravila društva
 - standardne klauzule EU-a o zaštiti osobnih podataka itd.
- (4) Umijeće jamstva koristi se kao mjerilo za odabir pružatelja usluga. Odluka Komisije o primjerenosti smatra se pouzdanim jamstvom; treba imati na umu da se odgovarajuće odluke o primjerenosti mogu razlikovati u svojem opsegu od zemlje do zemlje. Obvezujuća pravila društva također se mogu smatrati još jednim snažnim jamstvom.
- (5) SZOP mora unaprijed biti uključen u svaki prijenos/obradu izvan EU-a/EGP-a.
- (6) Društvo PHOENIX čuva dokaze o prijenosu osobnih podataka bilo kojemu pružatelju koji izvan EU-a/EGP-a.

1.22 6.3 Pravila za druge pružatelje usluga

Bilo koji treći pružatelji usluga i ugovorni suradnici koji izravno pristupaju podatkovnoj imovini uključujući osobne podatke u vlasništvu ili pod izravnom kontrolom PHOENIX Grupe moraju se prema ugovoru uskladiti s ovim Pravilnikom i obvezati se na povjerljivost.

7. OSTVARIVANJE PRAVA ISPITANIKA

- (1) OUZP daje sljedeća prava pojedincima:

- a) **pravo na informiranje**
Ispitanik dobiva bitne podatke u trenutku prikupljanja osobnih podataka ili prvom mogućom prilikom.
 - b) **pravo na pristup**
Ispitanik ima pravo zatražiti potvrdu o tomu obrađuju li se podaci koji se odnose na njega i, ako je to slučaj, zatražiti informacije u vezi s tim podacima u skladu s čl. 15. OUZP-a.
 - c) **pravo na ispravak**
Ispitanik ima pravo zatražiti dopunu ili ispravak netočnih podataka koji se odnose na njega.
 - d) **pravo na brisanje**
Ispitanik ima pravo zahtijevati brisanje svojih osobnih podataka ako ne postoje zakonske obveze čuvanja tih podataka.
 - e) **pravo na ograničenje obrade**
Ispitanik može zahtijevati ograničenje obrade u skladu s čl. 18. OUZP-a.
 - f) **pravo na prenosivost podataka**
Ispitanik ima pravo zatražiti kopiju svojih osobnih podataka koje Društvo PHOENIX čuva te usto zahtijevati da se oni prenesu drugim voditeljima obrade osobnih podataka.
 - g) **pravo na prigovor**
Ispitanik ima pravo uložiti prigovor u bilo kojemu trenutku na obradu svojih osobnih podataka, naročito radi izravnoga marketinga, profiliranja i istraživanja.
- (2) Društvo PHOENIX osigurava, odgovarajućim tehničkim i/ili organizacijskim mjerama, da može ispuniti prava ispitanika. Mjere se moraju dokumentirati.

Primjer: IT sustavi trebaju se odabrati ili osmisliti tako da se svi osobni podaci koji se odnose na ispitanika mogu ispisati kako bi se ispunito pravo na pristup ili se mora provesti postupak koji osigurava da se svi osobni podaci koji se odnose na osobu mogu ručno izvući iz sustava.

- (3) Ako se ispitanik obrati Društvu PHOENIX i zatraži ostvarivanje svojega prava kao ispitanika, dotični zaposlenik odmah prosljeđuje zahtjev SZOP-u i/ili slijedi daljnja lokalna pravila.

8. TEHNIČKE MJERE ZA ZAŠTITU OSOBNIH PODATAKA

Ukoliko se zadane postavke za obradu osobnih podataka mogu napraviti u sustavu, utoliko se te postavke moraju napraviti tako da se, s obzirom na svrhe upotrebe, ne obrađuje više podataka nego što je potrebno, ne dulje nego što je potrebno i ne sveobuhvatnije nego što je potrebno, a pristup je trećim stranama ograničen što je više moguće.

9. IZVJEŠĆIVANJE O POVREDI OSOBNIH PODATAKA

1.23 9.1 Interno izvješćivanje

- (1) Svaka povreda osobnih podataka mora se odmah prijaviti SZOP-u:

a) putem portala grupe PHOENIX:

<https://phoenixgroup-databreach.integrityplatform.org/>

ILI

b) putem lokalnoga alata/postupka.

Primjeri:

- *Gubitak poslovnoga mobilnoga telefona / prijenosnoga računala ili podatkovnoga medija*
 - *Korespondencija s pogrešnim primateljem*
 - *Neovlašten pristup korisničkomu portalu ili Speakapu*
 - *Zaraza sustava zlonamjernim softverom s učinkom na osobne podatke*
- (2) SZOP i LKS stvaraju zajednički postupak kako bi osigurali izvješćivanje. SZOP i LKS zajedno su odgovorni za podizanje svijesti o izvješćivanju o povredi osobnih podataka u Društvu PHOENIX.
- (3) VZOPD treba sudjelovati ako je povreda osobnih podataka međunarodna ili masovna (visok rizik za privatnost ispitanika ili pravni rizik za grupu PHOENIX).

1.24 9.2 Upravljanje povredom osobnih podataka

- (1) Na temelju internoga izvješća, SZOP određuje odgovornu osobu/odjele. Odgovorni zaposlenici/menadžeri čine *ad hoc* radnu skupinu sa SZOP-om. U kritičnu slučaju, odjel za komunikacije i Uprava također se pridružuju radnoj skupini.
- (2) Radna skupina ispituje činjenice slučaja i provodi procjenu rizika za pogođene ispitanike (kupci, zaposlenici itd.) i za Društvo PHOENIX.
- (3) Radna skupina odlučuje o mogućim mjerama za ublažavanje rizika i o obavijesti nadzornomu tijelu i/ili ispitanicima. Ova se odluka mora ispuniti u roku od 72 sata (prema saznanjima o povredi osobnih podataka) i mora se slijediti ovaj protokol:

Društvo PHOENIX (ni)je dužno dati službenu obavijest:		
NEMA RIZIKA za ispitanika = nema obveze obavješćivanja	RIZIK ZA PRAVA ispitanika = obavijest nadzornomu tijelu u roku od 72 sata	VISOK RIZIK ZA PRAVA ispitanika = obavijest nadzornomu tijelu u roku od 72 sata = obavijest ispitaniku u roku od 72 sata ili bez nepotrebna odgađanja.
U svakomu slučaju, radna skupina mora dokumentirati povredu osobnih podataka.		

- (4) O ovoj odluci SZOP obavješćuje Upravu. SZOP je u skladu s pravilima o obavješćivanju lokalnoga nadzornoga tijela.
- (5) SZOP i LKS stvaraju zajednički detaljan postupak kako bi osigurali upravljanje povredama osobnih podataka na lokalnoj razini.

10. PROVEDBENE AKTIVNOSTI

1.25 10.1 Provedbene aktivnosti društva

- (1) Pravilnici na razini cijele grupe, standardi zaštite osobnih podataka društva i predlošci društva predstavljaju glavne provedbene aktivnosti zaštite osobnih podataka društva.
- (2) Pravilnik koji je izradio odjel za zaštitu osobnih podataka društva dokument je koji navodi posebne zahtjeve ili pravila koja se moraju zadovoljiti, a koja je odobrio Izvršni odbor.
- (3) Standard zaštite osobnih podataka društva nije pravilnik, već najmanja standardna aktivnost, postupak ili alat koji je stvorio ili osigurao odjel za zaštitu osobnih podataka društva u skladu

- s pravilnikom o zaštiti osobnih podataka (**Standard**). Odobrenje Izvršnoga odbora nije potrebno. Standard ne utječe na Pravilnik, ali je alat za njegovu provedbu.
- (4) Zbirka standarda zaštite osobnih podataka društva jest vodič za zaštitu osobnih podataka društva (**Vodič ZOPD**).
 - (5) VZOPD priprema konačni Standard u skladu sa savjetovanjem s relevantnim dionicima društva i/ili SZOP-ima, ako je potrebno. VZOPD objavljuje Standard SZOP-ovima i uključenim dionicima društva. SZOP-ovi i uključeni dionik odgovorni su za daljnje objavljivanje ili prosljeđivanje Standarda relevantnim primateljima.
 - (6) Sljedeći dionici određeni su na razini grupe za Pravilnik na razini cijele grupe ili standarde zaštite osobnih podataka društva (ovisno o temi):
 - glavni službenik za sigurnost informacija
 - arhitekt informatičkih sustava
 - ured GSI-a
 - pravni odjel
 - odjel za reviziju
 - odjel opće nabave
 - odjel ljudskih resursa
 - (7) Društvo PHOENIX primjenjuje Standard na odgovarajući način (npr. lokalni pravilnik, uputa, tehnička prilagodba) uzimajući u obzir pravne ili organizacijske lokalne specifičnosti. Lokalna prilagodba može se postaviti na mjestu, ali ne smije prouzročiti da razina zaštite osobnih podataka padne ispod Standarda. Lokalna pravila o privatnosti ili tehnička rješenja moraju uvijek predstavljati najbolju moguću zaštitu osobnih podataka i na odgovarajući način zaštititi privatnost ispitanika. SZOP izvještava VZOPD-a godišnje ili na zahtjev o lokalnoj provedbi u državnim izvješćima.
 - (8) Predložak društva predstavlja najbolju praksu zaštite osobnih podataka u grupi PHOENIX.

1.26

1.27 10.2 Koncept zaštite osobnih podataka društva

Glavne provedbene aktivnosti društva grade sljedeći koncept zaštite osobnih podataka društva (**Koncept društva**). SZOP ovaj Koncept društva koristi za vlastite mjere i lokalne provedbene aktivnosti:

Vrsta dokumenta	Naziv dokumenta/alata
Pravilnik (pravila koja se moraju poštovati)	- Pravilnik o zaštiti osobnih podataka cijele grupe PHOENIX - Ako je potrebno, daljnji pravilnici o temama zaštite osobnih podataka za cijelu grupu - Pravilnici o informacijskoj sigurnosti (osiguravanje cjelovitosti i povjerljivosti osobnih podataka). <i>Odobrio Izvršni odbor</i> <i>Također dio lokalnoga koncepta</i>
Ugovori o grupnoj obradi podataka i ugovori o zajedničkim	Ishod pregovora unutar grupe <i>Odobrili Izvršni odbor i lokalna Uprava</i> <i>Također dio lokalnoga koncepta</i>

voditeljima obrade u grupi	
Standardi zaštite osobnih podataka društva <i>(najmanji standard za aktivnost, postupak ili alat u PHOENIX Grupi)</i>	Primjeri • Standard međunarodnoga prijenosa osobnih podataka • Standard životnoga ciklusa za koncept zaštite osobnih podataka: • Standard PUZOP-a • Standard koncepta zadržavanja • Sustav izvješćivanja o povredi osobnih podataka • Grupna mrežna platforma za obuku
Podizanje svijesti	Kampanja za podizanje svijesti u grupi

1.28 10.3 Koncept lokalne zaštite osobnih podataka

- (1) Lokalne provedbene aktivnosti grade lokalni koncept zaštite osobnih podataka (Lokalni koncept). SZOP podržava Upravu pri određivanju sadržaja Lokalnoga koncepta. Okvir za Lokalni koncept jest sljedeći:

Vrsta dokumenta	Naziv dokumenta/alata
Lokalni pravilnici / SOP-ovi / Uputa	Lokalni pravilnik o zaštiti osobnih podataka (ako je potrebno) Lokalni propisi na temelju Vodiča ZOPD-a ili lokalni zakonski zahtjevi: • Pravilnik o PUP-u/PUZOP-u • Pravilnik o konceptu zadržavanja • Pravilnik o upravljanju/izvješćivanju o povredi osobnih podataka • Pravilnik o vođenju evidencije o aktivnostima obrade • Pravilnik o ostvarivanju prava ispitanika
Lokalni predlošci	Na temelju predložaka društva • Ugovor o obradi osobnih podataka • Kontrolni popisi za obavijest o privatnosti • Letci
TOM-ovi	• Grupni ili lokalni pravilnici o informacijskoj sigurnosti • Formalna i neformalna dokumentacija (npr. koncept sigurnosne kopije, dnevnika itd.)
Podizanje svijesti	Lokalna kampanja za obuku i podizanje svijesti