Preview

GENERAL INFORMATION

edit

100%

Preview

Editing :	Daniel Bara	**Status :**	Simple validation
Evaluation :	Daniel Bara		
Validation :	Katarina Sunara		

Validation

Risk mapping

Risk seriousness

Risk likelihood

- Planned or existing measures
- With the corrective measures implemented
- (I)llegitimate access to data
- (U)nwanted modification of data
- (D)ata disappearance

5/31/21

Validation

Action plan

Overview

Fundamental principles

Purposes
Legal basis
Adequate data
Data accuracy
Storage duration
Information for the data subjects
Obtaining consent
Right of access and to data portability
Right to rectification and erasure
Right to restriction and to object
Subcontracting
Transfers

Planned or existing measures

Enkripcija
Anonimizacija
Particioniranje podataka
Kontrola logičkog pristupa
Arhiviranje
Papirnata dokumentacija
Smanjenje količine osobnih podataka
Operativna sigurnost
Suzbijanje zlonamjernog softvera
Upravljanje radnim stanicama
Sigurnost mrežnih stanica
Sigurnosne kopije
Održavanje
Ugovori o izvršavanju obrade
Mrežna sigurnost
Kontrola fizičkog pristupa
Praćenje aktivnosti mreže
Izbjegavanje izvora rizika
Zaštita od ne-ljudskih izvora rizika
Organizacija
Pravila
Upravljanje rizicima za privatnost
Integriranje zaštite privatnosti u projektima
Upravljanje povredama osobnih podataka
Upravljanje osobljem
Odnosi s trećim stranama
Nadzor
Pseudonimizacija
Lozinka
Autentifikacija
Filtriranje i ukljanjanje
Smanjenje osjetljivosti putem pretvorbe
Povreda osobnih podataka
Smanjenje identificirajuće prirode podataka
Ograničavanje pristupa podacima
Sljedivost i upravljanje zapisnicima

Risks

Illegitimate access to data
Unwanted modification of data
Data disappearance

Improvable Measures
Acceptable Measures

Fundamental principles

No action plan recorded.

Existing or planned measures

Enkripcija

Action plan / corrective actions :
U skladu s politikom čuvanjai arhiviranja, u godini u kojoj se dokumenti trebaju pobrisati, dok se ne pobrišu potrebno ih je enkriptirati ili anonimizirati, Također, je isto potrebno napraviti s transakijskim podacima na bazi koji sadrže osobne podatke. U komunickaiju putem e-mail omogućiti korištenje enkrptirane veze do računala kako bi se izbjegli rizici.
Evaluation comment :
Razmisliti o primjeni enkriptirane veze i u slučaju elektroničke pošte. Također, u zapisima na bazi potrebno je sagledati primjenu enkrpicije.
Expected date of implementation : 12/31/21
Responsible for implementation : IT

Anonimizacija

Action plan / corrective actions :
U skladu s politikom čuvanjai arhiviranja, u godini u kojoj se dokumenti trebaju pobrisati, dok se ne pobrišu potrebno ih je enkriptirati ili anonimizirati, Također, je isto potrebno napraviti s transakijskim podacima na bazi koji sadrže osobne podatke. U komunickaiju putem e-mail omogućiti korištenje enkrptirane veze do računala kako bi se izbjegli rizici.
Evaluation comment :
U kontekstu anonimiziranja dokumenata nema ekonomske opravdanosti za anonimiziranjem dokumenata ali u kontekstu eventualnog dugotrajnog čuvanja dokumenata u zapisima na bazi potrebno je sagledati primjenu anonimizacije.
Expected date of implementation : 12/31/21
Responsible for implementation : IT

Particioniranje podataka

Action plan / corrective actions :
Particionirati bazu na način da se podaci koji se odnose na medicinsku dokumentaciju spremaju logički na drugoj lokaciji.
Evaluation comment :
Razdijeliti podatke koji se odnose na medicinske
Expected date of implementation : 6/30/22
Responsible for implementation : IT

Kontrola logičkog pristupa

Action plan / corrective actions :
Izraditi dokument koji definira upravljanje logičkim pristupom informacijskom sustavu

Evaluation comment :
Jasno i formalno definiranje korisničkih profile, upravljanje poltikom zaporki, (minimalna duljina, zahtijevani znakovi, trajanje valjanosti, broj neuspjelih pokušaja prije zaključavanja pristupa računu i sl.).
Expected date of implementation : 7/31/21
Responsible for implementation : DPO, IT

Arhiviranje

Action plan / corrective actions :
Izraditi dokument koji formalno definira arhiviranje podataka
Evaluation comment :
Postupci su jasno definirani i u praksi se primjenjuju no nsu formalno zapisani.
Expected date of implementation : 12/31/21
Responsible for implementation : IT

Papirnata dokumentacija

Action plan / corrective actions :
Izraditi dokument koji formalno definira način ispisa, pohrane, uništavanja i razmjene papirnatih dokumenata. Npr. je li voditelj obrade u obavezi vratiti medicnski dokumentaciju ispitaniku? Da li se kod preuzimanja dokumentacije izrađuje zapisnik, iits.
Evaluation comment :
Postupci su jasno definirani i u praksi se primjenjuju no nisu formalno zapisani.
Expected date of implementation : 7/31/21
Responsible for implementation : DPO

Operativna sigurnost

Action plan / corrective actions :
Uvesati redovite mjesečne provjere stanja servera, mrežne opreme i ostalih komenenti informacijskog sustava koje održava administrator i u formi obrasca ih dostavljati voditelju obrade.
Evaluation comment :
U praksi administrator informacijskog sustava provodi nadzor, međutim to se radi ad-hoc i u slučaju eventualne sumnje. Potrebno je uvesti redovite mjesečne provjere i o tome obavještavati voditelja obrade putem zajednički definiranog obrasca.
Expected date of implementation : 12/31/21
Responsible for implementation : IT

Suzbijanje zlonamjernog softvera

Action plan / corrective actions :
Napraviti segmentaciju mreže i logički odvojiti pojedine segmente, npr. menadžment od ostatka tvrtke, te razmisliti o uvođenju DLP software no, prije toga napraviti analiziu rizika i sagledati potrebu za klasifikacijom podataka i dokumenata.
Evaluation comment :
U sustavu je implementirano dosta kontrola, no moguća su poboljšanja.
Expected date of implementation : 12/31/21
Responsible for implementation : IT

Upravljanje radnim stanicama

Action plan / corrective actions :
Uvesti redovito snimanje konfiguracija za pojedine važnije radne stanice i servere.
Evaluation comment :

Primijenjene kontrole su dobre, a za pojedine važnije radne stanice i servere je potrebno razmisliti snimanje konfiguracija. Primjena ažuriranja je adekvatna za veličinu sustava.
Expected date of implementation : 12/31/21
Responsible for implementation : IT

Ugovori o izvršavanju obrade

Action plan / corrective actions :
Realizirati aneks ugovora o zaštiti osobnih podataka
Evaluation comment :
Naknadno je utvrđeno kako još uvijek nije realiziran aneks ugovora za web hosting te je isti potrebno u nasjkorijem roku realizirati.
Expected date of implementation : 7/31/21
Responsible for implementation : UPRAVA

Zaštita od ne-ljudskih izvora rizika

Action plan / corrective actions :
Zamnijeniti postojeći UPS adekvatnim uređajem.
Evaluation comment :
UPS nije adekvatan
Expected date of implementation : 12/31/21
Responsible for implementation : IT

Upravljanje rizicima za privatnost

Action plan / corrective actions :
Izraditi rizike
Evaluation comment :
Izraditi rizike na osobne podatke
Expected date of implementation : 7/31/21
Responsible for implementation : DPO

Upravljanje povredama osobnih podataka

Action plan / corrective actions :
Revidirati predmetnu procuduru
Evaluation comment :
Proceduru je potrebno revidirati jer je od incijalnog dokumenta proteklo 3 godine
Expected date of implementation : 7/31/21
Responsible for implementation : DPO

Upravljanje osobljem

Action plan / corrective actions :
Uvesti odgovarajući pravilnik o radu, definirati disciplinske mjere u slučaju povrede osobnih podataka, uvesti redovite edukacije djelatnike
Evaluation comment :
Uvesti odgovarajući pravilnik o radu, definirati disciplinske mjere u slučaju povrede osobnih podataka, uvesti redovite edukacije djelatnike
Expected date of implementation : 12/31/21
Responsible for implementation : UPRAVA, DPO

Lozinka

Action plan / corrective actions :
Formalno definirati lozinku, čuvanje i pravila

Evaluation comment :
Uvesti formalnu definiciju lozinke
Expected date of implementation : 7/31/21
Responsible for implementation : IT

Autentifikacija

Action plan / corrective actions :
Razmisliti o primjeni dvorazinske autentifikacije npr. za VON pristup
Evaluation comment :
Nije primijenjena dvorazinska autentifikacija
Expected date of implementation : 12/31/21
Responsible for implementation : IT

Povreda osobnih podataka

Action plan / corrective actions :
Revidirati postojeću proceduru
Evaluation comment :
Postoji proicedura koju je potrebno revidirati.
Expected date of implementation : 7/31/21
Responsible for implementation : DPO

Sljedivost i upravljanje zapisnicima

Action plan / corrective actions :
Uvesti mjesečnu provjeru zapisa i o istoj izvještavati voditelja obrade.
Evaluation comment :
Nije definirana mjesečna provjera zapisa
Expected date of implementation : 12/31/21
Responsible for implementation : IT

Risks

No action plan recorded.

Validation

TO TRANSLATE - DPO and data subjects opinion

DPO's name

Daniel Bara

DPO's opinion

Predmetna obrada medicinske dokumentacije se može provoditi. Odabrane kontrole, rezidualni rizici i akcijski plan su prihvatljivi, s opravdanjima, s obzirom na prethodno utvrđene uloge i mišljenja dionika.

Search of concerned people opinion

Concerned people opinion wasn't requested.

Reason why concerned people opinion wasn't requested

Nije zatraženo mišljenje ispitanika jer je u njihovom interesu dostava medicinske dokumentacije kako bi voditelj obrade u njihovo ime i za njihov račun prikupio relevantne podatke za pokretanje, vođenje i zatvaranje odštetnog postupkaa

Context
Overview

What is the processing under consideration?

Prilikom obrade odštetnih zahtjeva prikuplja se medicinska dokumentacija oštećenika. Ova dokumentacija je nužna prilikom postupka.

What are the responsibilities linked to the processing?

Voditelj obrade ima odgovornost osigurati adekvatno spremanje dokumentacije, pristup samo odgovrnim osobama te zaštitu osobnih podataka ispitanika.

Are there standards applicable to the processing?

Ne postoje posebni standardi

Evaluation : Acceptable
Evaluation comment :
Nema posebnih standarda

Context
Data, processes and supporting assets

What are the data processed?

Obrađuju se zdravstveni podaci ispitanika koji uključuju:

Ime i prezime, adresu, OIB, MBO, broj osigurane osobe, telefonski broj, kao i medicinske podatke:
- Medicinska stanja
- Tretmani
- Planovi njege
- Tijekovi liječenja
- Korištenje lijekova
- Medicinska izvješća
- Planovi
- Rezultati ispitivanja, kao što su npr. rendgen, EKG UZV snimanja i laboratorijski testovi
- Pshihološki testovi

How does the life cycle of data and processes work?

U skladu s Politikom zadržavanja i uništavanja zapisa a u ovisnosti o vrsti odštetnog zahtjeva.

What are the data supporting assets?

Poslovna aplikacija i baze podataka skenirana dokumentacija

Evaluation : Acceptable
Evaluation comment :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Fundamental principles

Proportionality and necessity

Are the processing purposes specified, explicit and legitimate?

Da, u skladu je sa zakonom, posebna je i izričite.

Evaluation : Acceptable
Evaluation comment :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

What are the legal basis making the processing lawful?

Zakonska obaveza

Evaluation : Acceptable
Evaluation comment :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?

Da, podaci se koriste isključivo u vrshu dokumentacije potrebne prilikom obrade odštetnog zahtjeva i ne u potrebljavaju se za druge svrhe i to isključivo u mjeri koja je potrebna za određeni odštetni zahtjev.

Evaluation : Acceptable
Evaluation comment :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Are the data accurate and kept up to date?

Da, dokumentacija koja se prikuplja, posebno se prikuplja za predemetni odštetni zahtjev te mora biti točna i ažurna kako bi se ispunio zahtjev odštetnog predmeta.

Evaluation : Acceptable
Evaluation comment :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

What are the storage duration of the data?

Pohrana je u ovisnosti o vrsti odštetnog zahtjeva definirana u dokumentu Politika zadržavanja i uništavanja zapisa

Evaluation : Acceptable
Evaluation comment :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Fundamental principles

Controls to protect the personal rights of data subjects

How are the data subjects informed on the processing?

Ispitanik je obaviješten da je za otvaranje odštetnog zahtjeva u slučajevima kada je nužno prikupljanje medicinske dokumentacije, dužan dostaviti relevantnu, točnu i ažurnu medicinsku dokumentaciju. Bez relevantne dokumentacije nije moguće pokrenuti postupak odštete.

Evaluation : Acceptable
Evaluation comment :
Jasno iskomunicirano i definirano odgovarajućim dokumentima

If applicable, how is the consent of data subjects obtained?

Prilikom ugovaranja police osiguranja ispitanik je upoznat sa svojim pravima koja uključuju i prava prijave odštetnog zahtjeva. U slučaju odštetnog zahtjeva ispitanik je upoznat s činjenicom da za pokretanje odgovarajućeg postupka mora pribaviti relevantnu medicinsku dokumentaciju.

Evaluation : Acceptable
Evaluation comment :
Prema dostupnim informacijama, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

How can data subjects exercise their rights of access and to data portability?

Ispitanicima su prava regulirana u skladu sa Pravilnikom o zaštiti osobnih podataka i u svakom trenutku mogu ostvariti prava pristupa podacima.

Evaluation : Acceptable
Evaluation comment :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

How can data subjects exercise their rights to rectification and erasure?

Ispitanicima su prava regulirana u skladu sa Pravilnikom o zaštiti osobnih podataka i u svakom trenutku mogu ostvariti prava na ispravak i brisanje. Ukoliko je po predmetnom zahtjevu došlo do financijskih transkakcija koje uključuju eventualne podatke sa prikupljene medicisnke dokumentacije ispitanik se informira o toj činjenici i nemogućnosti brisanja takvih podataka zbog zakonske obaveze čuvanja.

Evaluation : Acceptable
Evaluation comment :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za

zaštitu podataka

How can data subjects exercise their rights to restriction and to object?

Ispitanicima su prava regulirana u skladu sa Pravilnikom o zaštiti osobnih podataka i u svakom trenutku mogu ostvariti prava na ograničenje i prigovor. Ispitanici su također informirani da ograničenje obrade znači i obustavu postupka pokretanja odštetnog zahtjeva

Evaluation : Acceptable
Evaluation comment :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Are the obligations of the processors clearly identified and governed by a contract?

Da, svi izvršitelji i podizvršitelji imaju potpisane ugovore ili su ugovori pri potpisu.

Evaluation : Acceptable
Evaluation comment :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

In the case of data transfer outside the European Union, are the data adequately protected?

Podaci se ne prenose izvan EU.

Evaluation : Acceptable
Evaluation comment :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Risks

Planned or existing measures

Enkripcija

Dokumentacija se dostavlja u digitalnom obliku a ako se dostavlja u papirnatom obliku, skenira se i u sprema u digitalnom obliku na u bazu . Papirnata dokumentacija se vraća klijentu ili se uništava. Dokumentacija nije kriptirana kao ni podaci na njoj. Podacima mogu pristupati kroz aplikaciju samo ovlašteni djelatnici. Ukoliko se dokumentacija dostavlja u digitalnom obliku putem elektroničke pošte sam put dokumentacije nije enkriptiran.

Evaluation : Improvable
Action plan / corrective actions :
U skladu s politikom čuvanjai arhiviranja, u godini u kojoj se dokumenti trebaju pobrisati, dok se ne pobrišu potrebno ih je enkriptirati ili anonimizirati, Također, je isto potrebno napraviti s transakijskim podacima na bazi koji sadrže osobne podatke. U komunickaiju putem e-mail omogućiti korištenje enkrptirane veze do računala kako bi se izbjegli rizici.
Evaluation comment :
Razmisliti o primjeni enkriptirane veze i u slučaju elektroničke pošte. Također, u zapisima na bazi potrebno je sagledati primjenu enkrpicije.

Anonimizacija

Anonimizacija se ne primjenjuje jer je predmetna dokumentacija u pdf ili doc formatu dostavljena voditelju obradu te je nepraktično i poslovno neopravdano implementirati je.

Evaluation : Improvable
Action plan / corrective actions :
U skladu s politikom čuvanjai arhiviranja, u godini u kojoj se dokumenti trebaju pobrisati, dok se ne pobrišu potrebno ih je enkriptirati ili anonimizirati, Također, je isto potrebno napraviti s transakijskim podacima na bazi koji sadrže osobne podatke. U komunickaiju putem e-mail omogućiti korištenje enkrptirane veze do računala kako bi se izbjegli rizici.
Evaluation comment :
U kontekstu anonimiziranja dokumenata nema ekonomske opravdanosti za anonimiziranjem dokumenata ali u kontekstu eventualnog dugotrajnog čuvanja dokumenata u zapisima na bazi potrebno je sagledati primjenu anonimizacije.

Particioniranje podataka

Podaci se nalaze na dijeljenoj datoteci zajedno sa drugim odacima i nisu posebno particionirani

Evaluation : Improvable
Action plan / corrective actions :
Particionirati bazu na način da se podaci koji se odnose na medicinsku dokumentaciju spremaju logički na drugoj lokaciji.
Evaluation comment :
Razdijeliti podatke koji se odnose na medicinske

Kontrola logičkog pristupa

Kontrola logičkog pristupa je definirana prilikom spajanja na poslovni sustav. Korisnik koji ima prava rada na računalu ujedno ima prava i rada u poslovnoj aplikaciji ali u onoj mjeri kako je to definirano poslovnom pozicijom. Pravila koja se primjenjuju na zaporke nisu posebno propisana iako se primjenjuju. Nije uvedeno zaključavanje nakon broja neuspjelih pokušaja, nije definirana valjanost. SSO ne postoji

Evaluation : Improvable
Action plan / corrective actions :
Izraditi dokument koji definira upravljanje logičkim pristupom informacijskom sustavu
Evaluation comment :
Jasno i formalno definiranje korisničkih profile, upravljanje poltikom zaporki, (minimalna duljina, zahtijevani znakovi, trajanje valjanosti, broj neuspjelih pokušaja prije zaključavanja pristupa računu i sl.).

Arhiviranje

Sva dokumentacije se arhivira i na backup server. Podaci ne spadaju unutar javnih okvira. Cijela baza svaki dan SQL skripta na drugi disk na istom serveru i na Synology. Backup prema Setcoru na drugoj lokaciji - Jastrebarsko.

Evaluation : Improvable
Action plan / corrective actions :
Izraditi dokument koji formalno definira arhiviranje podataka
Evaluation comment :
Postupci su jasno definirani i u praksi se primjenjuju no nsu formalno zapisani.

Papirnata dokumentacija

Papirnata dokumentacija

Dio dokumentacije se prikuplja u papirnatom obliku nakon čega se skenira te se papirnata dokumentacija vraća klijentu ili se uništava.

Evaluation : Improvable
Action plan / corrective actions :
Izraditi dokument koji formalno definira način ispisa, pohrane, uništavanja i razmjene papirnatih dokumenata. Npr. je li voditelj obrade u obavezi vratiti medicnski dokumentaciju ispitaniku? Da li se kod preuzimanja dokumentacije izrađuje zapisnik, iits.
Evaluation comment :
Postupci su jasno definirani i u praksi se primjenjuju no nisu formalno zapisani.

Smanjenje količine osobnih podataka

Prikupljanje dokumentacije je ugovorno i zakonski definirano te se prikupljaju podaci koji su nužni za pokretanje i provedbu odštetnog zahtjeva.

Evaluation : Acceptable
Evaluation comment :
Za informacijsku sustav voditelja obrade primijenjene kontrole su adekvatne.

Operativna sigurnost

Ne postoje dokumentirana posebna pravila koja bi bila uvedena kako bi se smanjila mogućnost i učinak rizika na sredstva koja podupiru osobne podatke iako se u praksi primjenjuju.

Evaluation : Improvable
Action plan / corrective actions :
Uvesati redovite mjesečne provjere stanja servera, mrežne opreme i ostalih komenenti informacijskog sustava koje održava administrator i u formi obrasca ih dostavljati voditelju obrade.
Evaluation comment :
U praksi administrator informacijskog sustava provodi nadzor, međutim to se radi ad-hoc i u slučaju eventualne sumnje. Potrebno je uvesti redovite mjesečne provjere i o tome obavještavati voditelja obrade putem zajednički definiranog obrasca.

Suzbijanje zlonamjernog softvera

Voditelj obrade koristi antivirusni softver Bit Defender a koriste i Bit Locker za enkripciju Hard diskova na svim laptopima. Ne postoji poseban DLP softver, nije uvedena segmentacija mreže, niti logičko odvajanje mrežnih segmenata.

Evaluation : Improvable
Action plan / corrective actions :
Napraviti segmentaciju mreže i logički odvojiti pojedine segmente, npr. menadžment od ostatka tvrtke, te razmisliti o uvođenju DLP software no, prije toga napraviti analiziu rizika i sagledati potrebu za klasifikacijom podataka i dokumenata.
Evaluation comment :
U sustavu je implementirano dosta kontrola, no moguća su poboljšanja.

Upravljanje radnim stanicama

Radne stanice se zaključavaju automatski nakon određenog vremena - 5 minuta. Ažuriranje se na radnim stanicama provodi kroz automatsko ažuriranje i nema centralnog nadzora ažuriranja. Konfiguracije računala a niti servera se ne spremaju posebno.

Evaluation : Improvable
Action plan / corrective actions :
Uvesti redovito snimanje konfiguracija za pojedine važnije radne stanice i servere.
Evaluation comment :
Primijenjene kontrole su dobre, a za pojedine važnije radne stanice i servere je potrebno razmisliti snimanje konfiguracija. Primjena ažuriranja je adekvatna za veličinu sustava.

Sigurnost mrežnih stanica

Osiguravanje mrežnih stanica je na osnovnoj razini. Postoji Clavister. Sav internet promet prolazi preko Setcora. Promet emaila je preko Setcora - email flow (prolazi filtere, antispam, av)

Evaluation : Acceptable
Evaluation comment :
Za informacijsku sustav voditelja obrade primijenjene kontrole su adekvatne.

Sigurnosne kopije

Postoje sigurnosne kopije baze podataka poslovne aplikacije, email sustava ali se ne rade posebne sigurnosne kopije radnih stanica. Nema potrebe jer se čuva na one drive pa zato i ne rade

Evaluation : Acceptable
Evaluation comment :
Za informacijsku sustav voditelja obrade primijenjene kontrole su adekvatne.

Održavanje

Nema posebno uvedenih pravila akoj bi definirala fizičko održavanje hardvera, hardver se održava ad-hoc i po potrebi. Održavanje je podugovorena kao reaktivno. Dopušteno je daljinsko održavanje aplikacija u skladu s ugovorom. Ne postoji posebno definirani postupak upravljanja s defektnom i rashodovanom opremom.

Evaluation : Acceptable
Evaluation comment :
Za informacijsku sustav voditelja obrade primijenjene kontrole su adekvatne.

Ugovori o izvršavanju obrade

Sa svim izvršiteljima obrade koji sudjeluju u procesu obrade osobnih podataka potpisani su odgovarajući aneksi ugovora o zaštiti osobnh podataka.

Evaluation : Improvable
Action plan / corrective actions :
Realizirati aneks ugovora o zaštiti osobnih podataka
Evaluation comment :
Naknadno je utvrđeno kako još uvijek nije realiziran aneks ugovora za web hosting te je isti potrebno u nasjkorijem roku realizirati.

Mrežna sigurnost

Voditelj obrade ima implementiranu privatnu mrežu kao i vatrozid, definirano preko Setcora.

Evaluation : Acceptable
Evaluation comment :
Za informacijsku sustav voditelja obrade primijenjene kontrole su adekvatne.

Kontrola fizičkog pristupa

Kontrola fizičkog pristupa nije posebno formalizirana. Posjetitelji ne mogu nez nadzora ući u prostorije voditelja obrade. Ulazna vrata kao i vrata server sobe su zaključana, a server soba je pod posebnim ključem, te ima svoju kameru. Implementiran je alarmni sustav koji reagira u slučaju provale. Protuprovala i smoke detektori su implementirani.

Evaluation : Acceptable
Evaluation comment :
Za informacijsku sustav voditelja obrade primijenjene kontrole su adekvatne.

Praćenje aktivnosti mreže

Prati se internet promet, lokalni ne, a Setcor prati svoj promet.

Evaluation : Acceptable
Evaluation comment :
Za informacijsku sustav voditelja obrade primijenjene kontrole su adekvatne.

Izbjegavanje izvora rizika

Potresi, poplave itd.? Za razgovro. DR u Jaski.

Evaluation : Acceptable
Evaluation comment :
Za informacijsku sustav voditelja obrade primijenjene kontrole su adekvatne. DR je realiziran u DC Jastrebarsko

Zaštita od ne-ljudskih izvora rizika

Implementirani dim detektori
UPS postoji ali je u postupku zamjene.

Evaluation : Improvable
Action plan / corrective actions :
Zamnijeniti postojeći UPS adekvatnim uređajem.
Evaluation comment :
UPS nije adekvatan

Organizacija

Podugovoren je eksternalizirani službenik za zaštitu podataka (DPO), a voditelj obrade je interno imenovao osobu za komunikaciju sa DPO-om

Evaluation : Acceptable
Evaluation comment :
Za informacijsku sustav voditelja obrade primijenjene kontrole su adekvatne.

Pravila

Definirano kroz Pravilnik o zaštiti osobnih podataka

Evaluation : Acceptable
Evaluation comment :
Za informacijsku sustav voditelja obrade primijenjene kontrole su adekvatne.

Upravljanje rizicima za privatnost

Voditelj obrade je u postupku izrade karte rizika

Evaluation : Improvable
Action plan / corrective actions :
Izraditi rizike
Evaluation comment :
Izraditi rizike na osobne podatke

Integriranje zaštite privatnosti u projektima

DPO je uključen u sve nove projekte kako bi se integrirala zaštita podataka u poslovanje

Evaluation : Acceptable
Evaluation comment :
DPO je uključen u sve aktivne projekte

Upravljanje povredama osobnih podataka

Definirano kroz Proceduru u slučaju povrede osobnih podataka

Evaluation : Improvable
Action plan / corrective actions :
Revidirati predmetnu procuduru
Evaluation comment :
Proceduru je potrebno revidirati jer je od incijalnog dokumenta proteklo 3 godine

Upravljanje osobljem

Tvrtka je u postupku izrade odgovarajućih dokumenata koji će upravljati podizanjem svijesti kod djelatnika

Evaluation : Improvable
Action plan / corrective actions :
Uvesti odgovarajući pravilnik o radu, definirati disciplinske mjere u slučaju povrede osobnih podataka, uvesti redovite edukacije djelatnike
Evaluation comment :
Uvesti odgovarajući pravilnik o radu, definirati disciplinske mjere u slučaju povrede osobnih podataka, uvesti redovite edukacije djelatnike

Odnosi s trećim stranama

Za svaki legitimni interes voditelj izrađuje test ranoteže kako bi se zaštitili interesi ispitanika

Evaluation : Acceptable
Evaluation comment :
Odgovarajući testovi se izrađuju.

Nadzor

Osoba zadužena za komunikaciju s DPO-om u obavezi je redovito mjesečno izvještavati o aktivnostima na području zaštite osobnih podataka

Evaluation : Acceptable
Evaluation comment :

Nadzor se redovito provodi.

Pseudonimizacija

Voditelj obrade za ovu specifičnu obradu nije predvidio pseudonimizaciju zbog nepraktičnosti promjena koje bi se trebale obavljati na digitalnim pdf skeniranim dokumentima.

Evaluation : Acceptable
Evaluation comment :
Nema opravdanog ekenomskog razloga za primjenu pseudonimizacije na medicisnku dokumentaciju

Lozinka

Lozinke moraju biti sastavljene od najmanje osam znakova; moraju se obnoviti ako postoji najmanja zabrinutost da bi one mogli biti ugrožene, a eventualno i povremeno (svakih šest mjeseci ili jednom godišnje) i moraju sadržavati najmanje tri od četiri vrste znakova (velika slova, mala slova, brojevi i posebni znakovi); kada se promijeni lozinka, posljednjih pet lozinki ne smiju se ponovno koristiti; istu lozinku ne smije se koristiti za različite pristupe; lozinke ne bi trebale biti povezane s osobnim podacima (uključujući ime ili datum rođenja). Odredite maksimalni broj pokušaja nakon kojih se izdaje upozorenje i autentikacija blokira (privremeno ili dok se ručno ne deblokira). Nema posebno definiranih formalnih pravila koa ovih navedenih

Evaluation : Improvable
Action plan / corrective actions :
Formalno definirati lozinku, čuvanje i pravila
Evaluation comment :
Uvesti formalnu definiciju lozinke

Autentifikacija

Svaka osobna se autentificira na računalo na kojem radi kroz AD. Nema dvorazinske autentifikacije

Evaluation : Improvable
Action plan / corrective actions :
Razmisliti o primjeni dvorazinske autentifikacije npr. za VON pristup
Evaluation comment :
Nije primijenjena dvorazinska autentifikacija

Filtriranje i ukljanjanje

Prilikom uvođenja dokumenata voditelj ne prikuplja metapodatke kao što su EXIF, lokacijski podaci i sl.

Evaluation : Acceptable
Evaluation comment :
Ne prikupljaju se navedeni metapodaci

Smanjenje osjetljivosti putem pretvorbe

Prikupljena medicinska dokumentacija se ne može pseudonimizirati niti pretvoriti u drugi oblik dok se ne završi postupak odštetnog zahtjeva koji u pojedinim slučajevim može biti dugotrajan (više godina). Nakon završetka postupka dokumentacija se može izbrisati, no u ovom trenutku voditelj obrade to ne radi.

Evaluation : Acceptable

Evaluation comment :
Nije moguće korištenje dokumentacije u drugom obliku osim onog koji se sprema u informacijski sustav

Povreda osobnih podataka

Definiran u okviru posebne Procedure u slučaju povrede osobnih podataka

Evaluation : Improvable
Action plan / corrective actions :
Revidirati postojeću proceduru
Evaluation comment :
Postoji proicedura koju je potrebno revidirati.

Smanjenje identificirajuće prirode podataka

Korisnik ne može koristiti resurs ili uslugu bez rizika otkrivanja identiteta (anonimnih podataka) zbog prirode dokumenata.
Korisnik ne može izvršiti višestruku upotrebu resursa ili usluga bez rizika da se te različite upotrebe povezuju zajedno (podaci se ne mogu povezati)

Evaluation : Acceptable
Evaluation comment :
Nije moguće koristiti dokumentaciju bez jasne identifikacije

Ograničavanje pristupa podacima

Podacima mogu pristupati samo ovlaštene osobe koje imaju prava uvida u predmet

Evaluation : Acceptable
Evaluation comment :
Primijenjene kontrole su adkevatne.

Sljedivost i upravljanje zapisnicima

Zapisnici postoje i pregledavaju se po potrebi.

Evaluation : Improvable
Action plan / corrective actions :
Uvesti mjesečnu provjeru zapisa i o istoj izvještavati voditelja obrade.
Evaluation comment :
Nije definirana mjesečna provjera zapisa

Risks

Illegitimate access to data

What could be the main impacts on the data subjects if the risk were to occur?

Povreda osobnih podataka, Šteta, Izrugivanje, Sramoćenje, Osuda ukoliko se radi o javnoj osobi

What are the main threats that could lead to the risk?

Otuđenje medicinske dokumentacije, Nepažnja djelatnika pri rukovanju s dokumentacijom, Računalna pogreška

What are the risk sources?

Zaposlenici, Nepažljivi korisnik, Nepažljivi IT administrator sustava, Haker, Ovlaštena tvrtka treće strane koja koristi povlašteni pristup

Which of the identified planned controls contribute to addressing the risk?

Kontrola logičkog pristupa, Smanjenje količine osobnih podataka, Operativna sigurnost, Suzbijanje zlonamjernog softvera, Upravljanje radnim stanicama, Sigurnosne kopije, Održavanje, Ugovori o izvršavanju obrade, Mrežna sigurnost, Kontrola fizičkog pristupa, Upravljanje rizicima za privatnost, Integriranje zaštite privatnosti u projektima

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Važan, Ispitanici mogu imati značajne posljedice koje bi trebali biti u stanju nadvladati, ali s pravim i ozbiljnim poteškoćama. Na primjer:
- materijalne: zloupotreba novca koji nije nadoknađen, ciljana, jedinstvena i neponavljajuća, izgubljene mogućnosti (kućni zajam, odbijanje studija, stažiranja ili zapošljavanja, zabrana izlaska na ispit), gubitak stanovanja, gubitak zaposlenja itd.;
- moralne: ozbiljne psihičke bolesti (depresija, razvoj fobije), osjećaj invazije privatnosti s nepovratnim oštećenjem, žrtva ucjene, internetskog zlostavljanja i uznemiravanja itd.
- političke

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Ograničen, Odabrani izvori rizika bi teško mogli ostvariti prijetnju iskorištavanjem svojstava pomoćnih sredstava.

Evaluation : Acceptable
Evaluation comment :
Odabrani izvori rizika bi teško mogli ostvariti prijetnju iskorištavanjem svojstava pomoćnih sredstava.

Risks

Unwanted modification of data

What could be the main impacts on the data subjects if the risk were to occur?

Povreda osobnih podataka

What are the main threats that could lead to the risk?

Otuđenje medicinske dokumentacije, Nepažnja djelatnika pri rukovanju s dokumentacijom, Računalna pogreška

What are the risk sources?

Nepažljivi korisnik, Zaposlenici, Nepažljivi IT administrator sustava

Which of the identified controls contribute to addressing the risk?

Kontrola logičkog pristupa, Upravljanje radnim stanicama, Ograničavanje pristupa podacima, Sljedivost i upravljanje zapisnicima

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Ograničen, Ispitanici mogu naići na značajne neugodnosti, koje će moći nadvladati unatoč nekoliko poteškoća. Na primjer:
- gubitka ugleda koji rezultira fizičkom ili psihološkom odmazdom itd.;
- materijalne: primanje neželjene ciljane pošte koja bi mogla oštetiti ugled ispitanika, itd.;
- moralne: manje, ali objektivne psihološke boli, osjećaj invazije privatnosti bez nepovratne štete,

zastrašivanje na društvenim mrežama itd..

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Ograničen, Čini se da bi odabrani izvori rizika teško mogli ostvariti prijetnju iskorištavanjem svojstava pomoćnih sredstava (npr. krađa digitalnih dokumenata pohranjenih na zaštićenom serveru).

Evaluation : Acceptable
Evaluation comment :
Čini se mogućim da bi odabrani izvori rizika ostvarili prijetnju iskorištavanjem svojstava pomoćnih sredstava

Risks
Data disappearance

What could be the main impacts on the data subjects if the risk were to occur?

Osuda ukoliko se radi o javnoj osobi, Povreda osobnih podataka, Šteta

What are the main threats that could lead to the risk?

Nepažnja djelatnika pri rukovanju s dokumentacijom, Otuđenje medicinske dokumentacije

What are the risk sources?

Haker, Nepažljivi korisnik, Zaposlenici, Ovlaštena tvrtka treće strane koja koristi povlašteni pristup

Which of the identified controls contribute to addressing the risk?

Kontrola logičkog pristupa, Smanjenje količine osobnih podataka, Operativna sigurnost, Ograničavanje pristupa podacima, Ugovori o izvršavanju obrade

How do you estimate the risk severity, especially according to potential impacts and planned controls?

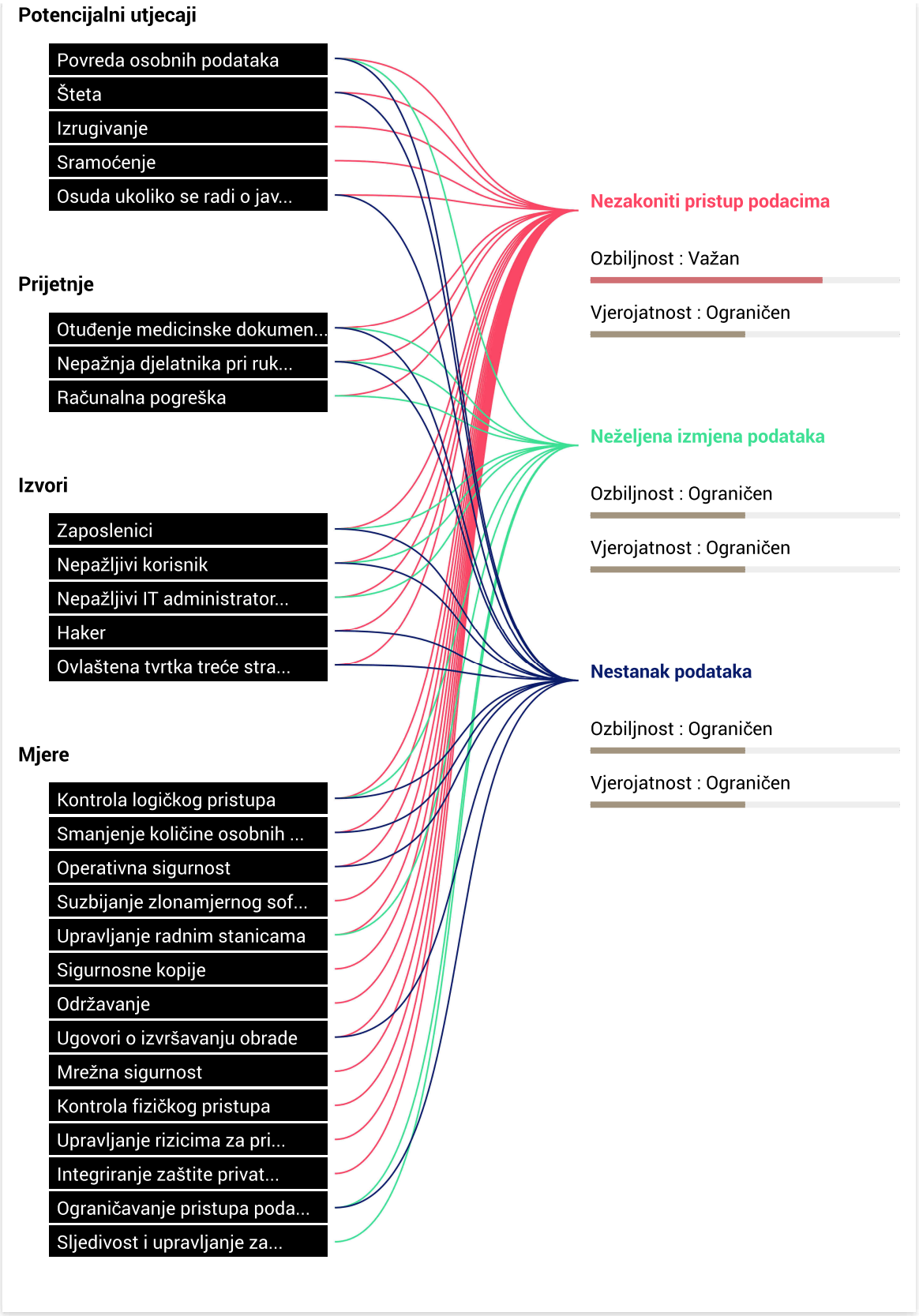
Ograničen, Ispitanici mogu naići na značajne neugodnosti, koje će moći nadvladati unatoč nekoliko poteškoća. Na primjer:
- fizičke: gubitka ugleda koji rezultira fizičkom ili psihološkom odmazdom itd.;
- materijalne: uskraćivanje pristupa administrativnim ili komercijalnim uslugama, primanje neželjene ciljane pošte koja bi mogla oštetiti ugled ispitanika, itd.;
- moralne: manje, ali objektivne psihološke boli, osjećaj invazije privatnosti bez nepovratne štete, zastrašivanje na društvenim mrežama itd..

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Ograničen, Čini se da bi odabrani izvori rizika teško mogli ostvariti prijetnju iskorištavanjem svojstava pomoćnih sredstava (npr. krađa digitalnih dokumenata pohranjenih na zaštićenom serveru).

Evaluation : Acceptable
Evaluation comment :
Čini se mogućim da bi odabrani izvori rizika ostvarili prijetnju iskorištavanjem svojstava pomoćnih sredstava.

Risks
Risks overview


Potencijalni utjecaji
Povreda osobnih podataka
Šteta
Izrugivanje
Sramoćenje
Osuda ukoliko se radi o jav...
Prijetnje
Otuđenje medicinske dokumen...
Nepažnja djelatnika pri ruk...
Računalna pogreška
Izvori
Zaposlenici
Nepažljivi korisnik
Nepažljivi IT administrator...
Haker
Ovlaštena tvrtka treće stra...
Mjere
Kontrola logičkog pristupa
Smanjenje količine osobnih ...
Operativna sigurnost
Suzbijanje zlonamjernog sof...
Upravljanje radnim stanicama
Sigurnosne kopije
Održavanje
Ugovori o izvršavanju obrade
Mrežna sigurnost
Kontrola fizičkog pristupa
Upravljanje rizicima za pri...
Integriranje zaštite privat...
Ograničavanje pristupa poda...
Sljedivost i upravljanje za...
Nezakoniti pristup podacima
Ozbiljnost : Važan
Vjerojatnost : Ograničen
Neželjena izmjena podataka
Ozbiljnost : Ograničen
Vjerojatnost : Ograničen
Nestanak podataka
Ozbiljnost : Ograničen
Vjerojatnost : Ograničen