TO TRANSLATE - Preview

uredi

100%

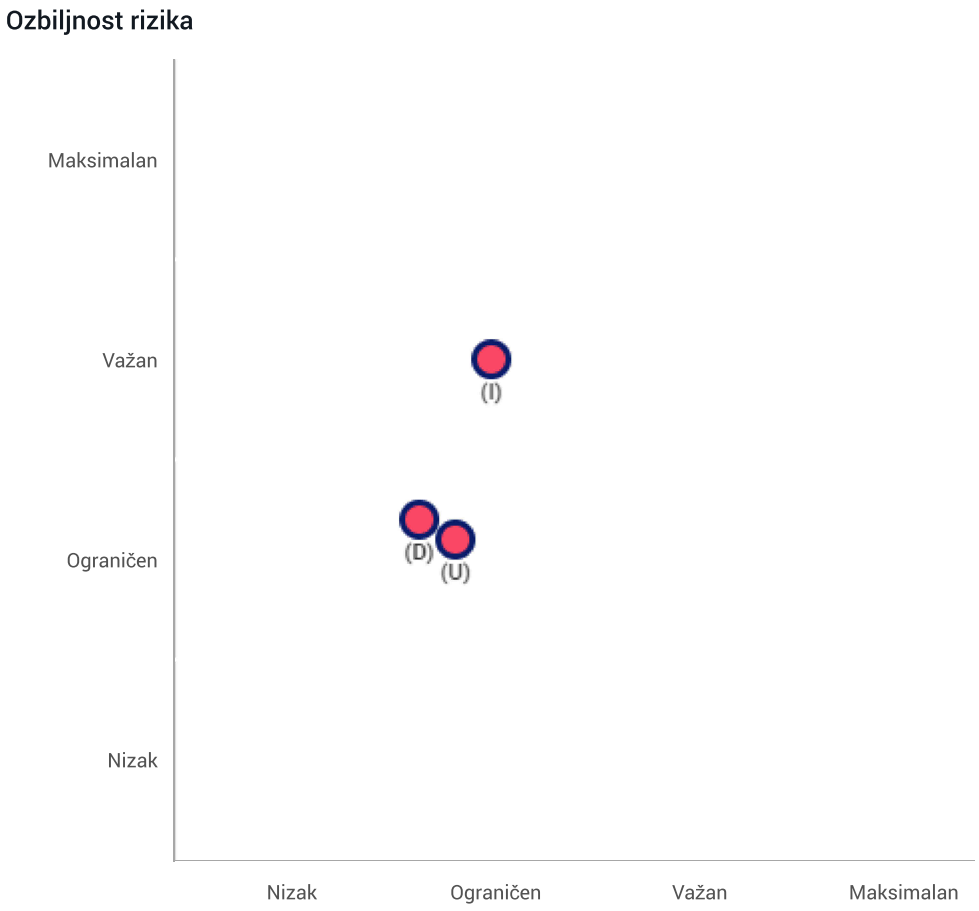
Kratki pregled

TO TRANSLATE - GENERAL INFORMATION

TO TRANSLATE - Editing :	Daniel Bara	**TO TRANSLATE - Status :**	Jednostavi potvrda
TO TRANSLATE - Evaluation :	Daniel Bara		
TO TRANSLATE - Validation :	Katarina Sunara		

TO TRANSLATE - Validation

Mapiranje rizika



- Postojeće ili planirane mjere
- Uz provođenje korektivnih mjera
- (N)ezakonit pristup podacima
- Neželjena (i)zmjena podataka
- Nestanak (p)odataka

31. 05. 2021.

TO TRANSLATE - Validation

Pregled

Temeljna načela

- Svrhe
- Pravna osnova
- Adekvatni podaci
- Točnost podataka
- Trajanje pohrane
- Informacije za ispitanike
- Dobivanje privole
- Pravo pristupa i prenosivosti podataka
- Pravo na ispravak i brisanje
- Pravo na ograničenje i prigovor
- Podugovaranje
- Prijenosi

Planirane ili postojeće mjere

- 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

Rizici

Nezakonit pristup podacima
Neželjena izmjena podataka
Nestanak podataka

Mjere Koje Se Daju Poboljšati
Prihvatljive Mjere

Temeljna načela

Nije zabilježen akcijski plan.

Postojeće ili planirane mjere

Enkripcija

Akcijski plan / aktivnosti ispravljanja :
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.
Komentar procjene :
Razmisliti o primjeni enkriptirane veze i u slučaju elektroničke pošte. Također, u zapisima na bazi potrebno je sagledati primjenu enkrpicije.
Očekivani datum provedbe : 31. 12. 2021.
Odgovoran za provedbu : IT

Anonimizacija

Akcijski plan / aktivnosti ispravljanja :
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.
Komentar procjene :
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.
Očekivani datum provedbe : 31. 12. 2021.
Odgovoran za provedbu : IT

Particioniranje podataka

Akcijski plan / aktivnosti ispravljanja :
Particionirati bazu na način da se podaci koji se odnose na medicinsku dokumentaciju spremaju logički na drugoj lokaciji.
Komentar procjene :
Razdijeliti podatke koji se odnose na medicinske
Očekivani datum provedbe : 30. 06. 2022.
Odgovoran za provedbu : IT

Kontrola logičkog pristupa

Kontrola logičkog pristupa

Akcijski plan / aktivnosti ispravljanja :
Izraditi dokument koji definira upravljanje logičkim pristupom informacijskom sustavu
Komentar procjene :
Jasno i formalno definiranje korisničkih profile, upravljanje poltikom zaporki, (minimalna duljina, zahtijevani znakovi, trajanje valjanosti, broj neuspjelih pokušaja prije zaključavanja pristupa računu i sl.).
Očekivani datum provedbe : 31. 07. 2021.
Odgovoran za provedbu : DPO, IT

Arhiviranje

Akcijski plan / aktivnosti ispravljanja :
Izraditi dokument koji formalno definira arhiviranje podataka
Komentar procjene :
Postupci su jasno definirani i u praksi se primjenjuju no nsu formalno zapisani.
Očekivani datum provedbe : 31. 12. 2021.
Odgovoran za provedbu : IT

Papirnata dokumentacija

Akcijski plan / aktivnosti ispravljanja :
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.
Komentar procjene :
Postupci su jasno definirani i u praksi se primjenjuju no nisu formalno zapisani.
Očekivani datum provedbe : 31. 07. 2021.
Odgovoran za provedbu : DPO

Operativna sigurnost

Akcijski plan / aktivnosti ispravljanja :
Uvesati redovite mjesečne provjere stanja servera, mrežne opreme i ostalih komenenti informacijskog sustava koje održava administrator i u formi obrasca ih dostavljati voditelju obrade.
Komentar procjene :
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.
Očekivani datum provedbe : 31. 12. 2021.
Odgovoran za provedbu : IT

Suzbijanje zlonamjernog softvera

Akcijski plan / aktivnosti ispravljanja :
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.
Komentar procjene :
U sustavu je implementirano dosta kontrola, no moguća su poboljšanja.
Očekivani datum provedbe : 31. 12. 2021.
Odgovoran za provedbu : IT

Upravljanje radnim stanicama

Akcijski plan / aktivnosti ispravljanja :
Uvesti redovito snimanje konfiguracija za pojedine važnije radne stanice i servere.
Komentar procjene :
Primijenjene kontrole su dobre, a za pojedine važnije radne stanice i servere je potrebno razmisliti snimanje konfiguracija. Primjena ažuriranja je adekvatna za veličinu sustava.
Očekivani datum provedbe : 31. 12. 2021.
Odgovoran za provedbu : IT

Ugovori o izvršavanju obrade

Akcijski plan / aktivnosti ispravljanja :
Realizirati aneks ugovora o zaštiti osobnih podataka
Komentar procjene :
Naknadno je utvrđeno kako još uvijek nije realiziran aneks ugovora za web hosting te je isti potrebno u nasjkorijem roku realizirati.
Očekivani datum provedbe : 31. 07. 2021.
Odgovoran za provedbu : UPRAVA

Zaštita od ne-ljudskih izvora rizika

Akcijski plan / aktivnosti ispravljanja :
Zamnijeniti postojeći UPS adekvatnim uređajem.
Komentar procjene :
UPS nije adekvatan
Očekivani datum provedbe : 31. 12. 2021.
Odgovoran za provedbu : IT

Upravljanje rizicima za privatnost

Akcijski plan / aktivnosti ispravljanja :
Izraditi rizike
Komentar procjene :
Izraditi rizike na osobne podatke
Očekivani datum provedbe : 31. 07. 2021.
Odgovoran za provedbu : DPO

Upravljanje povredama osobnih podataka

Akcijski plan / aktivnosti ispravljanja :
Revidirati predmetnu procuduru
Komentar procjene :
Proceduru je potrebno revidirati jer je od incijalnog dokumenta proteklo 3 godine
Očekivani datum provedbe : 31. 07. 2021.
Odgovoran za provedbu : DPO

Upravljanje osobljem

Akcijski plan / aktivnosti ispravljanja :
Uvesti odgovarajući pravilnik o radu, definirati disciplinske mjere u slučaju povrede osobnih podataka, uvesti redovite edukacije djelatnike
Komentar procjene :
Uvesti odgovarajući pravilnik o radu, definirati disciplinske mjere u slučaju povrede osobnih podataka, uvesti redovite edukacije djelatnike
Očekivani datum provedbe : 31. 12. 2021.
Odgovoran za provedbu : UPRAVA, DPO

Lozinka

Akcijski plan / aktivnosti ispravljanja :
Formalno definirati lozinku, čuvanje i pravila
Komentar procjene :
Uvesti formalnu definiciju lozinke
Očekivani datum provedbe : 31. 07. 2021.
Odgovoran za provedbu : IT

Autentifikacija

Akcijski plan / aktivnosti ispravljanja :
Razmisliti o primjeni dvorazinske autentifikacije npr. za VON pristup
Komentar procjene :
Nije primijenjena dvorazinska autentifikacija
Očekivani datum provedbe : 31. 12. 2021.
Odgovoran za provedbu : IT

Povreda osobnih podataka

Akcijski plan / aktivnosti ispravljanja :
Revidirati postojeću proceduru
Komentar procjene :
Postoji proicedura koju je potrebno revidirati.
Očekivani datum provedbe : 31. 07. 2021.
Odgovoran za provedbu : DPO

Sljedivost i upravljanje zapisnicima

Akcijski plan / aktivnosti ispravljanja :
Uvesti mjesečnu provjeru zapisa i o istoj izvještavati voditelja obrade.
Komentar procjene :
Nije definirana mjesečna provjera zapisa
Očekivani datum provedbe : 31. 12. 2021.
Odgovoran za provedbu : IT

Rizici

Nije zabilježen akcijski plan.

TO TRANSLATE - Validation

TO TRANSLATE - DPO and data subjects opinion

Ime SZP-a

Daniel Bara

Mišljenje SZP-a

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.

Traženje mišljenja dotičnih osoba

Nije zatraženo mišljenje dotične osobe.

Razlog zašto nije zatraženo mišljenje dotične osobe

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

Kontekst

Pregled

Koja je obrada koja se razmatra?

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

Koje su odgovornosti povezane s obradom?

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

Postoje li standardi primjenjivi na obradu?

Ne postoje posebni standardi

Procjena : Prihvatljiv
Komentar procjene :
Nema posebnih standarda

Kontekst

Podaci, procesi i pomoćna sredstva

Koji se podaci obrađuju?

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

Kako funkcionira životni ciklus podataka i postupaka?

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

O kojim se pomoćnim sredstvima radi?

O kojim se pomoćnim sredstvima radi?

Poslovna aplikacija i baze podataka skenirana dokumentacija

Procjena : Prihvatljiv
Komentar procjene :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Temeljna načela

Proporcionalnost i nužnost

Da li je svrha obrade posebna, izričita i zakonita?

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

Procjena : Prihvatljiv
Komentar procjene :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Koja je pravna osnova koja obradu čini zakonitom?

Zakonska obaveza

Procjena : Prihvatljiv
Komentar procjene :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Da li su prikupljeni podaci primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju ('smanjenje količine podataka')?

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.

Procjena : Prihvatljiv
Komentar procjene :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Jesu li podaci točni i ažurni?

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.

Procjena : Prihvatljiv
Komentar procjene :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Koliko je trajanje pohrane podataka?

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

Procjena : Prihvatljiv
Komentar procjene :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Temeljna načela

Kontrole radi zaštite osobnih prava nositelja podataka

Kako su voditelji obrade obaviješteni o obradi?

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.

Procjena : Prihvatljiv
Komentar procjene :
Jasno iskomunicirano i definirano odgovarajućim dokumentima

Ako je primjenjivo, kako se dobiva privola ispitanika?

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.

Procjena : Prihvatljiv
Komentar procjene :
Prema dostupnim informacijama, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Kako ispitanici mogu ostvariti svoja prava pristupa i prenosivosti podataka?

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

Procjena : Prihvatljiv
Komentar procjene :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Kako ispitanici mogu ostvariti svoja prava na ispravak i brisanje?

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.

Procjena : Prihvatljiv
Komentar procjene :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Kako ispitanici mogu ostvariti svoja prava na ograničenje i prigovor?

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

Procjena : Prihvatljiv
Komentar procjene :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Jesu li obveze izvršitelja obrade jasno identificirane i uređene ugovorom?

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

Procjena : Prihvatljiv
Komentar procjene :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

U slučaju prijenosa podataka izvan Europske unije, jesu li podaci primjereno zaštićeni?

Podaci se ne prenose izvan EU.

Procjena : Prihvatljiv
Komentar procjene :
Prema dostupnim informacijaa, primijenjene mjere dgovaraju pravilnom ispunjavanju zahtjeva za zaštitu podataka

Rizici

Planirane ili postojeće mjere

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.

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
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.
Komentar procjene :
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.

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
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.
Komentar procjene :
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

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
Particionirati bazu na način da se podaci koji se odnose na medicinsku dokumentaciju spremaju logički na drugoj lokaciji.
Komentar procjene :
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

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
Izraditi dokument koji definira upravljanje logičkim pristupom informacijskom sustavu
Komentar procjene :
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.

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
Izraditi dokument koji formalno definira arhiviranje podataka
Komentar procjene :
Postupci su jasno definirani i u praksi se primjenjuju no nsu formalno zapisani.

Papirnata dokumentacija

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

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
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.
Komentar procjene :
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.

Procjena : Prihvatljiv
Komentar procjene :
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.

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
Uvesati redovite mjesečne provjere stanja servera, mrežne opreme i ostalih komenenti informacijskog sustava koje održava administrator i u formi obrasca ih dostavljati voditelju obrade.
Komentar procjene :
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.

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
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.
Komentar procjene :
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 racunala a niti servera se ne spremaju posebno.

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
Uvesti redovito snimanje konfiguracija za pojedine važnije radne stanice i servere.
Komentar procjene :
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)

Procjena : Prihvatljiv
Komentar procjene :
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

Procjena : Prihvatljiv
Komentar procjene :
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.

Procjena : Prihvatljiv
Komentar procjene :
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.

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
Realizirati aneks ugovora o zaštiti osobnih podataka
Komentar procjene :
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.

Procjena : Prihvatljiv

Komentar procjene :
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.

Procjena : Prihvatljiv
Komentar procjene :
Za informacijsku sustav voditelja obrade primijenjene kontrole su adekvatne.

Praćenje aktivnosti mreže

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

Procjena : Prihvatljiv
Komentar procjene :
Za informacijsku sustav voditelja obrade primijenjene kontrole su adekvatne.

Izbjegavanje izvora rizika

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

Procjena : Prihvatljiv
Komentar procjene :
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.

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
Zamnijeniti postojeći UPS adekvatnim uređajem.
Komentar procjene :
UPS nije adekvatan

Organizacija

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

Procjena : Prihvatljiv
Komentar procjene :
Za informacijsku sustav voditelja obrade primijenjene kontrole su adekvatne.

Pravila

Definirano kroz Pravilnik o zaštiti osobnih podataka

Procjena : Prihvatljiv
Komentar procjene :

Komentar procjene :
Za informacijsku sustav voditelja obrade primijenjene kontrole su adekvatne.

Upravljanje rizicima za privatnost

Voditelj obrade je u postupku izrade karte rizika

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
Izraditi rizike
Komentar procjene :
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

Procjena : Prihvatljiv
Komentar procjene :
DPO je uključen u sve aktivne projekte

Upravljanje povredama osobnih podataka

Definirano kroz Proceduru u slučaju povrede osobnih podataka

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
Revidirati predmetnu procuduru
Komentar procjene :
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

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
Uvesti odgovarajući pravilnik o radu, definirati disciplinske mjere u slučaju povrede osobnih podataka, uvesti redovite edukacije djelatnike
Komentar procjene :
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

Procjena : Prihvatljiv
Komentar procjene :
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

Procjena : Prihvatljiv
Komentar procjene :
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.

Procjena : Prihvatljiv
Komentar procjene :
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

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
Formalno definirati lozinku, čuvanje i pravila
Komentar procjene :
Uvesti formalnu definiciju lozinke

Autentifikacija

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

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
Razmisliti o primjeni dvorazinske autentifikacije npr. za VON pristup
Komentar procjene :
Nije primijenjena dvorazinska autentifikacija

Filtriranje i ukljanjanje

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

Procjena : Prihvatljiv
Komentar procjene :
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.

Procjena : Prihvatljiv
Komentar procjene :
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

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
Revidirati postojeću proceduru
Komentar procjene :
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)

Procjena : Prihvatljiv
Komentar procjene :
Nije moguće koristiti dokumentaciju bez jasne identifikacije

Ograničavanje pristupa podacima

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

Procjena : Prihvatljiv
Komentar procjene :
Primijenjene kontrole su adkevatne.

Sljedivost i upravljanje zapisnicima

Zapisnici postoje i pregledavaju se po potrebi.

Procjena : Može se poboljšati
Akcijski plan / aktivnosti ispravljanja :
Uvesti mjesečnu provjeru zapisa i o istoj izvještavati voditelja obrade.
Komentar procjene :
Nije definirana mjesečna provjera zapisa

Rizici

Nezakoniti pristup podacima

Koji bi mogli biti glavni utjecaji na ispitanike ako se rizik pojavi?

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

Koje su glavne prijetnje koje bi mogle dovesti do rizika?

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

pogreška

Koji su izvori rizika

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

Koja od navedenih kontrola doprinosi odgovoru na rizik?

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

Kako procjenjujete ozbiljnost rizika , posebno prema potencijalnim utjecajima i planiranim kontrolama?

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

Kako procjenjujete vjerojatnost rizika , posebno u odnosu na prijetnje, izvore rizika i planirane kontrole?

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

Procjena : Prihvatljiv
Komentar procjene :
Odabrani izvori rizika bi teško mogli ostvariti prijetnju iskorištavanjem svojstava pomoćnih sredstava.

Rizici

Neželjena izmjena podataka

Koji bi mogli biti glavni utjecaji na ispitanike ako se rizik pojavi?

Povreda osobnih podataka

Koje su glavne prijetnje koje bi mogle dovesti do rizika?

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

Koji su izvori rizika ?

Nepažljivi korisnik, Zaposlenici, Nepažljivi IT administrator sustava

Koja od navedenih kontrola doprinosi odgovoru na rizik?

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

Kako procjenjujete ozbiljnost rizika , posebno u odnosu na potencijalne utjecaje i planirane kontrole?

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 poste koja bi mogla ostetiti ugled ispitanika, itd.;
- moralne: manje, ali objektivne psihološke boli, osjećaj invazije privatnosti bez nepovratne štete, zastrašivanje na društvenim mrežama itd..

Kako procjenjujete vjerojatnost rizika , posebno u odnosu na prijetnje, izvore rizika i planirane kontrole?

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

Procjena : Prihvatljiv
Komentar procjene :
Čini se mogućim da bi odabrani izvori rizika ostvarili prijetnju iskorištavanjem svojstava pomoćnih sredstava

Rizici

Nestanak podataka

Koji bi mogli biti glavni utjecaji na ispitanike ako se rizik pojavi?

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

Koje su glavne prijetnje koje bi mogle dovesti do rizika?

Nepažnja djelatnika pri rukovanju s dokumentacijom, Otuđenje medicinske dokumentacije

Koji su izvori rizika ?

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

Koja od navedenih kontrola doprinosi odgovoru na rizik?

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

Kako procjenjujete ozbiljnost rizika , posebno u odnosu na potencijalne utjecaje i planirane kontrole?

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..

Kako procjenjujete vjerojatnost rizika , posebno u odnosu na prijetnje, izvore rizika i planirane kontrole?

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

Procjena : Prihvatljiv
Komentar procjene :
Čini se mogućim da bi odabrani izvori rizika ostvarili prijetnju iskorištavanjem svojstava pomoćnih sredstava.

Rizici

Pregled rizika

Pregled rizika