Sigurnost, privatnost i arhitektura Virga ERP Cloud i Hatch! digitalnog programa vjernosti kupaca

Kompanijska posvećenost sigurnosti

Login d.o.o. je posvećen uspostavi međusobnog odnosa povjerenja i brige o vlastitim Korisnicima. Sastavni dio te misije je uspostava i održavanje pouzdanog upravljačkog okvira putem kojega uređujemo pitanja iz domene zaštite podataka za cjelokupnu paletu naših proizvoda i usluga, uključujući podatke Korisnika unešene tijekom korištenja naših usluga (Korisnički i Osobni podaci).

Pokrivene usluge

Ovaj dokument opisuje arhitekturu, provedene sigurnosne i nadzore zaštite privatnosti podataka, dobivene certifikate te organizacijske i tehničke zaštitne mjere primijenjene na Usluge pod tržišnim nazivima Virga ERP, Hatch! program vjernosti kupaca i Virga Loyalty digitalna platforma vjernosti kupaca smještene na infrastrukturi kojom upravlja Login d.o.o. (u daljnjem tekstu: Cloud)

Obrađivani podaci

Pokrivenim uslugama obrađuju se sljedeće vrste podataka:

Korisnički podaci – svi poslovni podaci Partnera nastali tijekom korištenja Usluge

Osobni podaci – svi osobni podaci Ispitanika koje Partner obrađuje temeljem zakonite osnove (Čl. 6.1(a-f))

Segregacija i pristup podacima

Pokrivene usluge funkcioniraju u višekorisničkom (multitenant) okruženju, dizajniranom sa ciljem odjeljivanja i ograničenja pristupa Korisničkim podacima na temelju poslovne potrebe za pristupom. Arhitektura omogućava efikasno logičko odjeljivanje (segregaciju) podataka različitih klijenata koristeći specifične identifikatore "vlasnika podataka", te pristupna prava temeljena na ulogama. Zaposlenici tvrtke Login d.o.o. i uključeni podizvršitelji pristupaju samo onim osobnim podacima u mjeri potrebnoj za obavljanje svojih poslovnih funkcija. Dodatna segregacija osigurana je korištenjem različitih okolina za različite funkcije, posebno za testna i produkcijska okruženja. Login d.o.o. ne dozvoljava instalaciju privatnog softvera ili drugog neodobrenog softvera na radne stanice i poslužitelje kompanije.

Infrastruktura – smještaj opreme

Pokrivene usluge smještene su u podatkovnim centrima kojima upravlja Login d.o.o., odnosno u kojima Login d.o.o. ima smještenu vlastitu računalnu opremu.

U smještaj opreme za pružanje **Pokrivenih usluga** uključene su sljedeće pravne osobe i podatkovni centri pod njihovim upravljanjem:

Vrsta resursa	Operater i država smještaja podatkovnog centra
Primarni produkcijski podatkovni centar	Login d.o.o., Hrvatska
Sekundarni (disaster-recovery) podatkovni centar	Altus informacijske tehnologije d.o.o., Hrvatska

Obrada Korisničkih i Osobnih podataka

U obradu **Korisničkih i Osobnih podataka** u svrhe koje se ne odnose na smještaj opreme uključene su sljedeće pravne osobe u svojstvu izvršitelja ili podizvršitelja obrade. Treće strane pružatelji usluge imaju pristup Korisničkim i Osobnim podacima temeljem prethodnog pristanka Korisnika te samo u opsegu potrebnom za pružanje tih usluga. Takvi pružatelji usluga mogu također imati pristup do sljedećih informacija o Korisniku u svrhu usmjeravanja i obrade zahtjeva za korisničkom podrškom: ime i prezime, email adresa, korisničko ime, broj telefona, adresa poslovnog nastana korisnika ili njegove izdvojene lokacije.

Naziv pravne osobe	Uloga	Država
Login d.o.o.	Izvršitelj obrade	Hrvatska
Login sustavi d.o.o.	Povezano društvo, podizvršitelj	Hrvatska
Istratech d.o.o.	Treća strana pružatelj usluge, podizvršitelj: Modularni informacijski sustav hotelijerstva i ugostiteljstva	Hrvatska
EBA d.o.o.	Treća strana pružatelj usluge, podizvršitelj: EBA DMS document management sustav	Slovenija

Kontrola obrade

Login d.o.o. je implementirao procedure kojima osigurava da se Korisnički i Osobni podaci obrađuju isključivo u okviru izvršenja aktivnosti definiranih ugovornim obavezama i temeljem pisanih uputa Korisnika, kroz cjelokupni tijek obrada koje obavlja tvrtka Login d.o.o. i/ili njezini podizvršitelji. Djelatnici tvrtke Login d.o.o., te drugi angažirani podizvršitelji, ugovorno su obavezani jamčiti provedbu odredbi privatnosti i zaštite podataka te primjene potrebnih sigurnosnih mjera zaštite s obzirom na svrhu i vrstu aktivnosti obrade. Ispunjavanje navedenih obaveza kao i provedba tehničkih i organizacijskih zaštitnih mjera od strane Login d.o.o. i njezinih podizvršitelja predmet su redovnih nadzora.

Funkcionalnosti trećih strana

Neke značajke Pokrivenih usluga koriste funkcionalnosti trećih strana. Korištenje takvih usluga je diskrecijsko pravo svakog Korisnika, pri čemu mjere opisane ovim dokumentom obuhvaćaju Pokrivene usluge samo u onom dijelu u kojem se njihova obrada vrši na dijelu infrastrukture kojom upravlja Login d.o.o ili njezini podizvršitelji.

Nadzorni pregledi i certifikacije

Certifikati sukladnosti opisani u nastavku ovog poglavlja primjenjuju se na Pokrivene usluge smještene na infrastrukturi kojom upravlja tvrtka Login d.o.o. Vlastita infrastruktura Korisnika, kao i smještaj u nekom od javnih cloud servisa nisu uključeni u opseg dolje opisanih certifikata.

- **ISO 27001 certifikacija**: Login d.o.o. je uspostavio i održava sustav upravljanja informacijskom sigurnošću (ISMS) za Pokrivene usluge u skladu sa zahtjevima ISO 27001 međunarodnog standarda upravljanja informacijskom sigurnošću. Certifikacijski nadzor provodi nezavisna treća strana. Dobiveni ISO 27001 certifikat i Izjava o primjenjivosti dostupni su na zahtjev ovlaštenoj osobi korisnika.

Pokrivene usluge podložne su dodatnim internim provjerama ranjivosti infrastrukture i aplikativnih rješenja.

Sigurnosne mjere

Pokrivene usluge uključuju različite konfigurabilne postavke koje Korisnicima omogućuju prilagođavanje određenih postavki Pokrivenih usluga prema vlastitim potrebama, kao što su autentifikacija korisnika, pristupna prava i uloge, bilježenje log zapisa. Log zapisima bilježi se unos, izmjena ili brisanje Korisničkih i Osobnih podataka u sustavima tvrtke Login d.o.o. ili njegovih podizvršitelja.

Sigurnosne politike i procedure

Pokrivene usluge pružaju se u skladu sa sljedećim politikama i procedurama kako bi se poboljšala razina sigurnosti:

- Kao dio Politike informacijske sigurnosti, osobni podaci zahtijevaju najmanje istu razinu zaštite prilikom njihovog prijenosa, obrade i pohrane kroz internu mrežu tvrtke Login d.o.o. kao i "povjerljive" informacije, na način na koji je klasifikacija definirana Politikom upravljanja klasificiranim informacijama tvrtke Login d.o.o.
- Korisničke lozinke pohranjuju se korištenjem jednosmjernih hash funkcija
- Podaci o pristupima korisnika bilježe datum, vrijeme, korisničko ime, pozvani programski modul i/ili URL, vrstu aktivnosti (izrada, ažuriranje, brisanje), te izvornu (source) IP adresu i/ili naziv radne stanice ili pristupnog uređaja
- U slučaju sumnje u neovlašteni pristup tvrtka Login d.o.o. može dostaviti korisniku log zapise o pristupima za potrebe forenzičke analize
- Fizički logovi pristupa podatkovnom centru, sistemskoj infrastrukturi te logovi sa aplikativnih sustava čuvaju se minimalno 90 dana
- Lozinke se ne bilježe u log zapise
- Izvršitelj i podizvršitelji obrade ne postavljaju lozinke u ime korisnika. Lozinke su resetirane na slučajnu vrijednost (koja mora biti promijenjena prilikom prve prijave) te automatski dostavljene korisniku koji je zatražio promjenu putem elektroničke pošte.

Sustav za otkrivanje upada

Tvrtka Login d.o.o. ili ovlaštena treća strana, nadzirati će Pokrivene usluge u svrhu detekcije neovlaštenog upada korištenjem mrežno-baziranih ili računalno-baziranih sustava za otkrivanje upada. Login d.o.o. može analizirati podatke prikupljene od strane korisničkih internet preglednika (npr. vrsta uređaja, rezolucija zaslona, vremenska zona, verzija operativnog sustava, vrsta i verzija preglednika, korišteni MIME tipovi, i dr.) zbog sigurnosnih razloga, uključujući detekciju kompromitiranih web preglednika, neovlaštene prijave te osiguranja ispravnog rada Pokrivenih usluga.

Sistemski log zapisi

Sva oprema korištena u pružanju Pokrivenih usluga, uključujući vatrozid (firewall), usmjerivače, mrežne preklopnike i operativne sustave, bilježe informacije na odgovarajuće lokacije ili centralizirani syslog sustav u svrhu provođenja sigurnosnih pregleda, analize i posjedovanja evidencije za slučaj sigurnosnih incidenata.

Upravljanje incidentima

Tvrtka Login d.o.o. ima uspostavljene politike i procedure upravljanja sigurnosnim incidentima. Login d.o.o. će bez nepotrebnog odgađanja obavijestiti obuhvaćene Korisnike čim sazna za povredu Osobnih podataka koje u ime Korisnika obrađuje tvrtka Login d.o.o. i angažirani podizvršitelji, uključujući slučajno ili namjerno uništenje, gubitak, promjenu, neovlašteno otkrivanje ili pristup podacima.

Tvrtka Login d.o.o. uobičajeno obavještava korisnike u slučaju značajnih incidenata ili problema u radu sustava putem emaila. U slučaju većih neplaniranih incidenata Login d.o.o. može informirati korisnike o štetnom događaju i planu rješavanja korištenjem drugih prikladnih načina komunikacije.

Autentifikacija korisnika i pristup sustavima

Pristup Pokrivenim uslugama zahtijeva autentifikaciju korištenjem jednog od podržanih mehanizama autentifikacije, uključujući korisničko ime/lozinku, 2-factor autentifikaciju, Oauth, prijavu putem društvenih mreža. Slučajni identifikator (ID) korisničke sesije generira se i pohranjuje u korisnički web preglednik ili drugi klijentski alat nakon uspješne autentifikacije te služi za pohranu i praćenje stanja korisničke sesije. Pristup sustavima odobrava se isključivo temeljem prethodnog odobrenja ovlaštenih osoba, te se tako dobivene autorizacije i pristupna prava povlače nakon prestanka za njihovom potrebom, uključujući odlazak osobe na drugo radno mjesto ili napuštanje tvrtke. Pristup računalnoj mreži tvrtke zaštićen je od pristupa sa javne mreže firewall uređajem. Primjenjuju se sigurnosne zakrpe kako bi se osigurala redovita i periodična instalacija potrebnih sigurnosnih nadogradnji. Potpuni udaljeni pristup internoj mreži Logina štićen je sigurnom VPN vezom.

Fizička sigurnost

Podatkovni centri korišteni za pružanje Pokrivenih usluga koriste kontrole pristupa koje omogućuju samo ovlaštenim osobama ulaz u sigurne zone. Te lokacije dizajnirane su sa ciljem da budu otporne na vremenske nepogode i druge razumno predvidljive uvjete, koriste redundantne električne i

telekomunikacijske vodove, sustave za nadzor temperature, vlage i drugih radnih uvjeta u prostoru smještaja opreme, kao i protuprovalne i vatrodojavne sustave. Sustavi neprekidnog napajanja i pomoćni agregati koriste se u slučaju prekida isporuke električne energije.

Pouzdanost i sigurnosne kopije podataka

Mrežne komponente, web poslužitelji i aplikacijski poslužitelji konfigurirani su u redundantnom načinu rada. Korisnički podaci pohranjeni su na primarni poslužitelj baze podataka. Za pohranu podataka koristi se visoko redundantni diskovni podsustav sa višestrukim putevima pristupa kojima se osigurava pouzdanost i performanse rada sustava. Korisnički i Osobni podaci unešeni u sustav korištenjem Pokrivenih usluga, do zadnje potvrđene transakcije, automatski se repliciraju uz manji vremenski odmak na sekundarnu lokaciju. Na primarnoj lokaciji redovito se izrađuju sigurnosne kopije podataka (backup).

Oporavak od ispada (disaster recovery)

Podatkovni centri dizajnirani su na način da budu otporni na jedinstvene slabe točke ispada te osiguraju kontinuitet rada i potrebne performanse. Pokrivene usluge koriste sekundarnu lokaciju, zemljopisno udaljenu od primarnog podatkovnog centra, uključujući potrebnu strojnu opremu, programsku podršku i veze prema internetu za slučaj neplanirane dostupnosti primarne lokacije.

Pokrivene usluge trenutno imaju sljedeće ciljeve oporavka: (a) restauraciju Pokrivenih usluga (recovery time objective) unutar 24 sata od proglašanja ispada od strane tvrtke Login d.o.o.; i (b) maksimalni gubitak podataka (recovery point objective) od 4 sata. Navedeni ciljevi ne primjenjuju se u slučaju katastrofe ili više katastrofa čiji nastup istovremeno kompromitira oba podatkovna centra u isto vrijeme te ne uključuju razvojna i testna okruženja.

Računalni virusi

Pokrivene usluge ne nadziru mogućnost postojanja virusa u učitanim prilozima ili drugim podacima pohranjenima kroz Pokrivene usluge od strane Korisnika. Pohranjeni prilozi se ne izvršavaju u okviru Pokrivenih usluga te stoga ne mogu oštetiti ili kompromitirati Pokrivene usluge u slučaju sadržavanja virusa. Interna računalna mreža Logina sustavi d.o.o., zaštićena je antivirusnim softverom na svim ulaznim točkama mreže (e-mail računi), kao i na svim datotečnim poslužiteljima i radnim stanicama.

Podatkovna enkripcija

Pokrivene usluge koriste industrijski prihvaćene enkripcijske produkte za zaštitu podataka te njihov prijenos između korisničke mreže i Pokrivenih usluga, uključujući minimalno 128-bit TLS certifikate i 2048-bit RSA javni ključ. Dodatno, svi podaci, prenose se za potrebe replikacije podataka između podatkovnih centara koristeći AES-256 enkripciju.

Povrat Korisničkih podataka

U roku od 60 dana od dana prestanka važenja Ugovora o korištenju **Pokrivene usluge**, Korisnici mogu zatražiti povrat podataka unešenih tijekom korištenja Pokrivenih usluga (osim podataka prethodno obrisanih od strane Korisnika). Tvrtka Login d.o.o. će omogućiti preuzimanje podataka u strojno čitljivom formatu te eventualne priloge u njihovom izvornom formatu.

Brisanje Korisničkih podataka

Nakon isteka svih važećih licenci vezanih uz korištenje Pokrivenih usluga, Korisnički podaci uneseni kroz korištene usluge biti će zadržani u statusu mirovanja u periodu do najviše 180 dana, nakon čega će biti izbrisani/uništeni na siguran način. Fizički mediji pohrane na kojima su tijekom korištenja usluge pohranjeni podaci neće biti fizički uklonjeni iz podatkovnih centara koje koristi tvrtka Login d.o.o. za pohranu podataka, osim ukoliko je medij došao do kraja svojeg funkcionalnog ciklusa, u kojem slučaju će medij biti uništen sigurnim putem. Taj postupak je podložan važećoj zakonskoj regulativi. Ne umanjujući mogućnost Korisnika da zatraži povrat Korisničkih podataka unesenih tijekom korištenja Pokrivenih usluga, Login d.o.o. zadržava pravo smanjenja perioda retencije podataka nakon prestanka važenja Ugovora o korištenju **Pokrivene usluge**. Login d.o.o. će takvu izmjenu objaviti u ovom dokumentu.

Analitika

Tvrtka Login d.o.o. može pratiti i analizirati korištenje Pokrivenih usluga u cilju povećanja sigurnosti sustava te poboljšanja Pokrivenih usluga i korisničkog iskustva u korištenju Pokrivenih usluga kroz praćenje trendova, te poboljšanje funkcionalnosti često korištenih modula i funkcionalnosti.