Ugovor o obradi podataka

Privitak 1: **Koncept zaštite podataka**

Stanje: Verzija 2.6, 08.11.2024
Kontakt osoba: Matthias Menne, Službenik za zaštitu podataka onOffice GmbH

Uvod

Privitak 1 opisuje tehničke i organizacijske mjere prema članku 32. GDPR koje trebaju osigurati sigurnost obrade koja je obuhvaćena ugovorom:

- Implementacija online CRM softverskog rješenja onOffice enterprise
- Hosting web stranica
- Import podataka
- Prijenos podataka
- Hosting E-Mailova

Mnoge obrade odvijaju se na istim IT sustavima i uz iste sigurnosne mjere. Stoga će na početku svakog poglavlja biti opisane ove zajedničke sigurnosne mjere, nakon čega ćemo se usredotočiti na pojedine obrade.

Šifriranje

Mrežni promet od i prema onOffice enterpriseu je osiguran HTTPS-om. Podržane su verzije TLS-a 1.2 i 1.3.

Web stranice se mogu osigurati certifikatima verificiranim od strane CA “Let’s Encrypt”, San Francisco CA, SAD.

Mediji poslani u okviru uvoza podataka bit će šifrirani prije povratka klijentu.

Prilikom slanja E-Maila koristi se TLS sa Perfect Forward Security, ukoliko ga serverska strana primaoca podržava.

Povjerljivost

Povjerljivost osobnih podataka osigurava se time što samo ovlaštene osobe imaju fizički ili logički pristup.

Kontrola pristupa

Ako nije drugačije naznačeno, sve obrade se odvijaju u podatkovnom centru Telehouse Deutschland GmbH (vidi privitak 2).

Ovdje postoji kontrola pristupa putem beskontaktnog identifikacijskog sustava, 24/7 nadzor od strane osiguranja i video nadzor. Pravo pristupa pojedinim prostorijama sa serverima programirano je posebno za svaku prostoriju.

Sigurnosne kopije se pohranjuju u prostorijama koje je Telehouse Deutschland GmbH unajmio u podatkovnom centru Equinix (Germany) GmbH u Düsseldorfu.

Zaposlenici oba podatkovna centra nemaju pristup pohranjenim podacima.

U poslovnim prostorima onOffice GmbH u Aachenu, osobni podaci naručitelja čuvaju se samo kratkotrajno za interne softverske testove (ako je apsolutno nužno) ili za import podataka. Davanje ključeva zaposlenicima se dokumentira. Izvan radnog vremena, poslovni prostori su osigurani alarmnim sustavom, a u slučaju alarma automatski se obavještava služba za nadzor.

Mediji poslani unutar okvira importa podataka čuvaju se sigurno u poslovnim prostorima. Raspoloživost medija se dokumentira pismeno. Import podataka se izvodi na serveru u poslovnim prostorima tvrtke onOffice GmbH u Aachenu. Server se nalazi u posebnoj server sobi koja je osigurana alarmnim sustavom, evidencijom pristupa i video nadzorom.

Kontrola prilaza

Pristup onOffice enterprise/smart sustavu je moguć isključivo unosom točnog korisničkog imena, imena aktivnog i neblokiranog korisnika i ispravne lozinke. Prilikom unosa, korisničko ime i lozinka nisu vidljivi. Koliko često korisnici trebaju mijenjati lozinke može postaviti korisnik s administratorskim ovlastima putem softvera. Složenost lozinke se automatski provjerava prilikom unosa nove lozinke; ako ne odgovora određenoj vrijednosti, lozinka se neće prihvatiti.

Pristup produktivnim sustavima je ograničen na apsolutno nužan krug osoba i osiguran Public-Private-Key-Autentifikacijom. Prilikom završetka poslovanja onOffice zaposlenika, pristupi se brišu.

Standardni softver instaliran na serverima redovito se provjerava radi sigurnosno kritičnih ažuriranja. Nakon toga se ažuriranja instaliraju što je brže moguće, uz očuvanje dostupnosti sustava.

Osobni podaci naručitelja se obrađuju od strane zaposlenika onOffice GmbH izvan poslovnih prostora samo ako je to nužno. U ovom slučaju se isto pridržava IT sigurnosna politika kao i unutar poslovnih prostora.

Mrežni promet se nadzire putem firewalla.

Kontrola pristupa

U onOffice enterprise/smart sustavu, pristup zapisima se može ograničiti na razini korisnika. Za to je potrebno dodijeliti određene zapise određenim korisnicima ili grupama te adekvatno ograničiti prava korisnika. Dodatno se može dodati modul koji omogućava postavljanje prava za čitanje i pisanje za pojedine kontakte / nekretnine / povijest zapisa za svakog korisnika. Korisnici mogu stvoriti popis podataka koje su nedavno otvorili.

E-Mail poštanski sandučići u onOffice enterprise/smart sustavu mogu se dodijeliti jednom ili više korisnika. Tada E-Mail poštanski sandučić nije više vidljiv drugim korisnicima.

Integritet

Izmjene podataka o kontaktima i nekretninama provedene u onOffice enterprise/smart sustavu se bilježe. Ove promjene mogu biti praćene od strane korisnika s administratorskim ovlastima.

onOffice enterprise/smart ima mogućnost podrške za više klijenata. Podaci svakog klijenta pohranjuju se u vlastitu bazu podataka. Korisniku nije moguće pregledavati podatke drugih verzija klijenata bez prijave u drugu verziju putem navedenog mandatnog imena, korisničkog imena i lozinke.

Izmjene u kodnoj osnovi onOffice enterprise/smart se pažljivo testiraju i tek nakon toga se stavljaju na raspolaganje ograničenom broju klijenata na nekoliko tjedana. Tek nakon toga se primjenjuju za sve klijente. Ispravci pogrešaka se primjenjuju za sve klijente dva puta tjedno, u hitnim slučajevima odmah.

Privitci u E-Mailovima se provjeravaju na viruse, a antivirusna zaštita za ostale obrade se provjerava ili već primjenjuje.

Dostupnost

Baze podataka klijenata se svake noći sigurnosnim kopijama kompletno pohranjuju. Sigurnosne kopije se pohranjuju u prostorijama koje je Telehouse Deutschland GmbH unajmio u podatkovnom centru Equinix (Germany) GmbH u Düsseldorfu (vidi privitak 2). Datoteke klijenata se jednom mjesečno sigurnosnim kopijama kompletno pohranjuju, dok se svake noći pohranjuju inkrementalnim sigurnosnim kopijama.

Iznimno od “Importa podataka” i “Prijenosa podataka”, sve obrade se provode u Telehouse podatkovnom centru. Dostupnost podataka osigurana je putem N+1 redundantnog napajanja izvanredne struje, zaštite od požara s optičkim / termalnim detektorima i Inergen sustavom gašenja te redundantnih mrežnih povezivanaj s više operatera.

Za sve obrade dostupna je dovoljno računalnog kapaciteta kako bi se izbalansirao pad više servera. Podaci klijenata pohranjeni su u RAID5 sustavu.

Radi zaštite od DDoS napada, onOffice sudjeluje u Prolexic mreži od Akamai-a. Svi upiti prema sustavima onOffice GmbH se preusmjeravaju preko servera tvrtke Akamai. Pri čemu se filtriraju upiti koji su dio DDoS napada.

Zakonitost obrade

Svi zaposlenici tvrtke onOffice GmbH su obvezni čuvati tajnost podataka i obučavaju se u području zaštite podataka i IT-sigurnosti.

Sa svim podizvođačima su sklopljeni ugovori o obradi podataka. Prije zaključenja ugovora, podizvođači se provjeravaju na prikladnost. Na taj način se jamči da su i zaposlenici podizvođača obvezani na čuvanje povjerljivih podataka.

Prilikom planiranja funkcionalnosti i procesa uvijek se uključuje princip minimizacije podataka (“Privacy by Design”).

Upravljanje zaštitom podataka

Koncept zaštite podataka se provodi putem radnih uputa, sporazuma i tehničko-organizacijskih mjera. Prikladnost koncepta zaštite podataka se provjerava najmanje jednom godišnje. Ako je potrebno, koncept zaštite podataka ili provedba koncepta zaštite podataka se prilagođava.

Upravljanje reakcijom na incidente

IT sustavi koji se koriste za obradu se neprekidno nadziru. U slučaju incidenata, pristup osobnim podacima se obnavlja što je brže moguće. Nakon incidenata, u okviru naknadne analize provjerava se treba li revidirati IT sigurnosni koncept ili IT plan za izvanredne situacije, te jesu li tehničko-organizacijske mjere i IT infrastruktura dovoljna da se spriječi incident iste vrste u budućnosti.

Obrada podataka u trećim zemljama

onOffice koristi Akamais Prolexic Network. Kako bi se osigurala optimalna zaštita od DDoS napada, promet prema sustavima tvrtke onOffice GmbH preusmjerava se preko servera diljem svijeta. Nadzor prometa provodi se u Sjedinjenim Američkim Državama. Stoga se, pod određenim uvjetima, sljedeći osobni podaci mogu obrađivati izvan Europske unije:

1. IP-adresa klijenta
2. domena koju je potražio
3. u slučaju neosiguranog http prometa: URL adresa

Akamai je po EU-US Data Privacy Framework certificiran.

onOffice je s Akamai-om zaključio EU standardne ugovorne klauzule u verziji od lipnja 2021., koristeći Modul 3 (Obrada i Obrada).