CCHBC Politika privatnosti podataka

1. Svrha politike, obim i faktori rizika

CCHBC je posvećen zaštiti ličnih podataka dobijenih u kontekstu svojih poslovnih aktivnosti, pridržavanje važećeg zakonodavnog i regulatornog okvira u vezi sa obradom ličnih podataka, čuvajući svoju reputaciju i konkurentnu tržišnu poziciju, štiti podatke svojih kupaca .

Ova politika definiše principe privatnosti i prakse koje se moraju primeniti u okviru Kompanije, uzimajući u obzir lokalne zakone i propise za zaštitu ličnih podataka.

Politika se primenjuje na sve oblike podataka, informacionih sistema, operacija i procesa u okruženju Kompanije koje uključuju prikupljanje, skladištenje, korišćenje i prenos ličnih podataka.

Ova politika se odnosi na sve zaposlene u Kompaniji i njenim filijalama širom sveta, kao i na sve poslovne partnere (kao što su dobavljači, izvođači, prodavci i drugi pružaoci usluga) koji primaju, šalju, prikupljaju, pristupaju ili obrađuju na bilo koji način lične podatke u ime Kompanije.

Faktor rizika: Nedostatak politike može dovesti do nenamernog kršenja procedura kompanije, neovlašćeno otkrivanje poverljivih informacija Kompanije ili narušen integritet ili oštećenje imovine Kompanije koje dovodi do gubitka konkurentske prednosti ili kršenja GDPR-a i drugih važećih zakona, izazivajući finansijski gubitak i/ili negativan uticaj na korporativni imidž Kompanije.

2. Izjava o politici

Preduzeće mora uspostaviti adekvatne organizacione i tehničke kontrole u cilju zaštite integritet poverljivost i dostupnost ličnih podataka, kako u digitalnom tako iu fizičkom formatu.

Politika zaštite podataka ne zamenjuje utvrđenu Politiku zaštite informacija i Politika prihvatljivog korišćenja, ali umesto toga dopunjuje ih sa tehničkim i organizacionim kontrolama uzimajući u obzir lične podatke u skladu sa zahtevima GDPR-a.

3. Svrha

Kompanija je uspostavila šemu klasifikacije podataka kao deo Politike zaštite informacija pod nazivom Politika klasifikacije informacija s obzirom na lične podatke.

Prema ovoj Politici, svi lični podaci moraju se smatrati poverljivim i kao takvi moraju biti adekvatno zaštićeni od neovlašćene upotrebe i/ili otkrivanja. Ova politika navodi posebna pravila u vezi sa prikupljanjem, skladištenjem, prenosom i odlaganjem takvih informacija kako bi se to osiguralo i fizičke i elektronske datoteke, kao i njihovi odgovarajući informacioni sistemi, su klasifikovani, označeni i efikasno zaštićeni.

4. Vlasništvo i revizija dokumenta

Vlasnik ovog dokumenta je Group Data Protection Officer (DPO). Ovaj dokument treba pregledati i, ako je potrebno, ažurirati najmanje jednom godišnje.

5. Odobrenja

Dokument odobrava Group Chief Information Security Officer (CISO).

6. Detalji politike

6.1. Prikupljanje podataka

Prikupljanje ličnih podataka mora biti tačno, relevantno i ograničeno na ono što je neophodno, u vezi u zakonite poslovne svrhe.

Kompanija mora izvršiti dodatne procese validacije kako bi osigurala da lični podaci prikupljeni su tačni i potpuni za poslovne svrhe za koje su namenjeni da se koriste.

Kompanija mora pregledati i osigurati da su svi metodi prikupljanja ličnih podataka pošteni i zakoniti, bez zastrašivanja i obmane, pridržavajući se zakona i propisa koji se odnose na prikupljanje ličnih podataka.

Štaviše, Kompanija mora da potvrdi da treća lica od kojih se prikupljaju lični podaci:

- Koristite poštene i zakonite metode prikupljanja informacija.
- Poštuju ovu Politiku i svoje ugovorne obaveze prema Kompaniji u pogledu prikupljanje, korišćenje i prenos ličnih podataka u ime Kompanije.

6.2. Ograničavanje upotrebe i otkrivanja trećim licima

Lični podaci se ne smeju koristiti ili otkrivati u druge svrhe osim onih prvobitnog prikupljanja osim ako imalac podataka nije izričito dao saglasnost ili kako to zahteva zakon.

Ako je potrebna saradnja sa novim dobavljačem kao procesorom podataka, Grupa za zaštitu podataka Kancelarija i, ako je primenjivo, lokalni koordinator za zaštitu podataka (DPO gde je primenjivo) moraju biti blagovremeni obavešteni i uključeni unapred kako bi se osiguralo da je proces evaluacije privatnosti po dizajnu sprovedeno tokom procesa izbora dobavljača i pre zaključenja ugovora sa dobavljač.

Ukoliko Kompanija prekine saradnju sa obrađivačem podataka koji je obradio lične podatke u ime Kompanije, onda organizacija mora osigurati da su svi lični podaci vraćeni ili trajno izbrisani, uništeni ili anonimizovani u prostorijama obrađivača podataka.

U određenim okolnostima, dozvoljeno je otkrivanje ličnih podataka agencijama za sprovođenje zakona bez saglasnost nosioca podataka. U ovim slučajevima, Kompanija može otkriti tražene podatke. Međutim, Kompanija mora da obezbedi da je zahtev legitiman i da se konsultuje sa pravnim savetnicima Kompanije ako neophodno.

6.3. Međunarodni prenos podataka unutar i van EEA

Kompanija je dizajnirala i uspostavila okvir koji pokriva prekogranični prenos podataka, uključujući adekvatne procedure za praćenje i/ili praćenje prekograničnih tokova podataka iz Evropske ekonomske Područje (EEP) u zemlju van EEP.

Pored toga, Kompanija će uvek obezbediti da se lični podaci ne prenose van Evropskog ekonomskog prostora (EEP), u treću zemlju koja nema adekvatne zahteve u pogledu uspostavljena zaštita podataka, bilo svojim domaćim zakonodavstvom ili međunarodnim obavezama, što je a član.

Ukoliko se lični podaci prenesu van EEP, Kompanija mora da obezbedi da je sporazum na mestu koje obezbeđuje da postoje odgovarajući mehanizmi prenosa i kontrole zaštite podataka mesto.

Ugovor koji obezbeđuje zaštitne mere u vezi sa ličnim podacima koji se prenose bilo kome

lokacija izvan EEP nije potrebna kada se primenjuje bilo šta od sledećeg:

- Pojedinci su dali saglasnost za prenos svojih informacija.
- Predložena destinacija je na beloj listi.

6.4. Skladištenje podataka

Lični podaci uskladišteni u fizičkom formatu, bazama podataka, čvrstim diskovima, laptopu ili bilo kom drugom elektronskom format mora biti adekvatno zaštićen od neovlašćenog pristupa, otkrivanja i/ili neovlašćenog pristupa.

Kompanija mora da sprovede odgovarajuće tehničke kontrole:

- Industrijski prihvaćeni standardi očvršćavanja za radne stanice, servere i baze podataka:
- Kompletno softversko šifrovanje diska na svim operativnim sistemima za radne stanice/laptop računare pogoni koji čuvaju lične podatke.
- Šifrovanje u mirovanju uključujući upravljanje ključem ličnim podacima van Kompanije prostorijama.
- Omogućite evidentiranje bezbednosne revizije u svim sistemima koji obrađuju lične podatke.
- Ograničite upotrebu prenosivih medija kao što su USB fleš diskovi.
- Tehnike anonimizacije u okruženjima za testiranje.
- Zakrpe softvera, sistema i aplikacija.
- Dvofaktorska autentikacija za korisnike i administratore koji pristupaju sistemima koji hostuju lične podataka.
- Kontrola fizičkog pristupa gde se lični podaci čuvaju u štampanoj kopiji.

6.5. Prenos podataka

Prilikom prenosa ili prenosa ličnih podataka, Kompanija mora da obezbedi da je to prikladno uspostavljene su organizacione i tehničke kontrole kako bi se zaštitila poverljivost i integritet podataka.

Kontrole moraju podržavati:

- Omogućite šifrovane komunikacione kanale preko kriptografskih protokola (TLS).
- Šifrovanje svih dolaznih/odlaznih veza.
- Obezbedite pristup na osnovu principa autentifikacije i autorizacije kompanije.
- Šifrovanje e-pošte i priloga koji sadrže lične podatke. Gde nisu dostupne, smernice pod uslovom da se prilozi sa lozinkom saopštavaju na posebnom komunikacija.
- Obezbedite obuku i svest zaposlenih i administratora da pažljivo upravljaju ličnim podatke koji se odnose na Kompaniju iu skladu sa Politikom prihvatljivog korišćenja kako biste izbegli:

- Lični podaci koji se šalju na adrese e-pošte koje nisu korporativne, kao što su Gmail ili Outlook.
- Lični podaci za otpremanje na ne-korporativne usluge u oblaku.
- Lični podaci koji se prenose usmeno ili pismeno neovlašćenim licima.

6.6. Usvajanje podataka

Preduzeće ima zakonsku obavezu da čuva određene evidencije u minimalnom vremenskom periodu. Kompanija ne sme čuvati lične podatke duže nego što je potrebno za ispunjenje identifikovanih zakonitih poslovnih ciljeva ili dokle god to zahteva važeći zakon.

Neophodno je da Kompanija uspostavi period čuvanja ličnih podataka u skladu sa relevantnim zakona i propisa kao dela evidencije aktivnosti obrade.

Kompanija mora da opravda zahteve za čuvanje ličnih podataka u periodima dužim od maksimalni period zadržavanja prema poslovnim i regulatornim zahtevima ako je potrebno.

Ukoliko Preduzeće zadrži lične podatke duži vremenski period u štampanim kopijama, onda da bi smanji rizik od fizičkog izlaganja, Kompanija mora da nastavi sa digitalizacijom arhive preko specijalizovanog i sertifikovanog provajdera treće strane.

Kompanija mora da zadrži ovu digitalizovanu arhivu u bezbednom okruženju gde su samo ovlašćeni osoblje ima pristup.

Gde je moguće, elektronski sistemi moraju biti podešeni da označavaju zapise za pregled/brisanje kada je to izvesno vremenski periodi su istekli u skladu sa periodima zadržavanja prema lokalnom zakonu.

6.7. Odlaganje podataka

Po isteku identifikovanih zakonitih poslovnih ciljeva ili povlačenju saglasnosti, Kompanija moraju ili bezbedno raspolagati ili anonimizirati lične podatke imalaca podataka na osnovu Bezbednih podataka Standard za odlaganje.

Da bi se obezbedila poverljivost podataka, svi fizički dokumenti koji sadrže lične podatke moraju biti na odgovarajući način odloženi korišćenjem šredera dokumenata.

Kompanija može da sarađuje sa spoljnim dobavljačem kako bi odložila ogromne količine papira dokumenti. U tom slučaju mora postojati ugovor o usluzi i zapisnik o uništenju zapisa moraju biti proizvedeni na odgovarajući način. Eksterni provajder mora biti izabran na osnovu specifičnih zahteva kako bi se demonstrirala usklađenost sa GDPR-om.

Za lične podatke koji se čuvaju na elektronskim medijima za skladištenje, Kompanija mora da koristi tehnike prepisivanja u kako bi se osiguralo da su podaci nepovratni.

Ukoliko Kompanija zadrži lične podatke duže od unapred definisanog ograničenja (npr.zadržati podatke u neproizvodnim okruženjima u svrhe testiranja), podaci moraju biti anonimizovani ili nepovratno anonimizovan kako bi se sprečila jedinstvena identifikacija pojedinca.

7. Istorija revizija

Revizija br	Datum objavljivanja	Autor revizije	Napomene
1st Version	April 16th 2018	Nassos Stylianos (Group DPO)	Creation
2nd Version	May 1st 2018	Waldo Scholtz Group Data & Analytics Director	Review
3rd Version	May 25th	Nassos Stylianos (Group DPO)	Review and Update
4th Version	October 19th	Nassos Stylianos (Group DPO)	Review and Update
5th Version	December 10 2020	Nassos Stylianos (Group DPO)	Review and Update
6th Version	July 1st 2021	Nassos Stylianos (Group DPO)	Review and Update
7th Version	December 7 2022	Nassos Stylianos (Group DPO)	Review
8th Version	December 14 2023	Nassos Stylianos (Group DPO)	Review and Update

8. Aneks A – Termini i definicije

Ovaj odeljak pruža definicije termina koji se obično koriste u ovoj Politici.

GDPR	Opšta uredba o zaštiti podataka
DPO	Službenik za zaštitu podataka
Lični podaci	Sve informacije koje se odnose na fizičko lice koje je identifikovano ili koje se može identifikovati(„imalac podataka“); fizičko lice koje se može identifikovati je ono koje se može identifikovati, direktno ili indirektno, posebno pozivanjem na identifikator kao što je ime, identifikacioni broj, podaci o lokaciji, onlajn identifikator ili na jedan ili više faktora specifičnih za fizičke, fiziološke, genetski, mentalni, ekonomski, kulturni ili društveni identitet tog fizičkog lica
Posebne kategorije ličnih podataka (osetljivi/sudski podaci)	Lični podaci koji su po prirodi posebno osetljivi u odnosu na osnovna prava i slobode i koji otkrivaju rasno ili etničko poreklo, politička mišljenja, verska ili filozofska uverenja, učešće u sindikatu, genetske i biometrijske podatke, zdravstvene podatke, seksualni život, seksualnu orijentaciju , osude i prestupima

Imalac podataka	Odnosi se na svakog pojedinca koji je imalac ličnih podataka koje drži Kompanija, kao što su zaposleni ili kupci
Rukovalac	Fizičko ili pravno lice, organ javne vlasti, agencija ili drugi organ koji samostalno ili zajedno sa drugima utvrđuje svrhe i sredstva obrade podataka o ličnosti; kada su svrhe i sredstva takve obrade utvrđeni zakonom unije ili države članice, rukovalac ili posebni kriterijumi za njegovo imenovanje mogu biti predviđeni pravom Unije ili države članice
Obrađivač podataka	Fizičko ili pravno lice, javni organ, agencija ili drugi organ koji obrađuje lične podatke u ime rukovaoca
ISM	Menadžer za bezbednost informacija
Kršenje ličnih podataka	Kršenje bezbednosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmene, neovlašćenog otkrivanja ili pristupa ličnim podacima koji se prenose, čuvaju ili na drugi način obrađuju
Treća strana	Sva eksterna pravna i fizička lica – uključujući bez ograničenja izvođače radova, prodavce, dobavljače usluga i partnere – koji imaju pristup informacionim sredstvima Kompanije, informacionim sistemima ili koji obrađuju korporativne informacije u ime Kompanije

9. Aneks B Imaoci podataka i kategorije ličnih podataka

Kompanija je uspostavila sledeće kategorije nosilaca podataka i ličnih podataka:

1. Kategorije imalaca podataka:

- Zaposleni
- Članovi porodice zaposlenih
- Bivši zaposleni
- Kandidata za posao
- Kupci
- Potrošači
- Deca i druge ugrožene grupe
- Prodavci
- Druge treće strane
- Zainteresovane strane

2. Kategorije ličnih podataka

- Opšti lični podaci: bilo koja informacija koja se odnosi na fizičko lice, identifikovano ili moguće identifikovati, takođe indirektno pozivanjem na bilo koju drugu informaciju, na primer, ime, prezime, e-mail adresa, grad.

- Osetljivi podaci: lični podaci koji otkrivaju rasno i etničko poreklo, verska uverenja, filozofska ili politička mišljenja, članstvo u sindikatu, zdravstveno stanje i seksualni život

- Sudski podaci: podaci pogodni za otkrivanje nezakonitog ili prevarantskog ponašanja, sudske mere ili postupaka i disciplinskih, administrativnih ili računovodstvenih mera ili postupaka

- Biometrijski podaci: lični podaci koji su rezultat specifične tehničke obrade u vezi sa fizičke, fiziološke karakteristike ili karakteristike ponašanja (u vezi sa fizičkom ili telesnom prirodom i isključujući ponašanje u marketinške svrhe koje je posebna kategorija u nastavku) od fizičko lice, koji dozvoljavaju ili potvrđuju jedinstvenu identifikaciju tog fizičkog lica,kao što su slike lica ili podaci o otiscima prstiju

- Podaci o ponašanju: podaci o ponašanju su sve vrste podataka prikupljenih o pojedincu ponašanje u marketinške svrhe. U kontekstu digitalnog marketinga, podaci o ponašanju su uglavnom prikupljeni na mreži, ali mogu doći i iz oflajn izvora.

Neke vrste podataka o ponašanju su:

- Podaci prikupljeni na bihevioralnim oglasnim mrežama (pregledanje i reakcije na oglase)

- Podaci o ponašanju prikupljeni na veb lokaciji

- Komentari i aktivnosti na veb stranicama društvenih medija

- Genetski podaci: označavaju „ lični podaci koji se odnose na naslednu ili stečenu genetiku karakteristike fizičkog lica koje daju jedinstvene informacije o fiziologiji ili zdravlje tog fizičkog lica i koji proizilaze , posebno, iz analize a biološki uzorak dotičnog fizičkog lica, posebno ” .