
Politika e Privatësisë së të Dhënave e CCHBC

1. Qëllimi i politikave, fushëveprimi dhe faktori i rrezikut

CCHBC (Kompania) angazhohet për mbrojtjen e të dhënave personale të fituara në kontekstin e aktiviteteve të saj të biznesit, duke respektuar kornizën legjislative dhe rregullatore, në lidhje me përpunimin e të dhënave personale dhe duke ruajtur reputacionin e saj dhe pozicionin konkurrues të tregut, duke ruajtur të dhënat e klientëve të tyre.

Politika në fjalë përcakton parimet dhe praktikën e privatësisë që duhet të zbatohen brenda kompanisë, duke marrë parasysh ligjet dhe rregulloret lokale për mbrojtjen e të dhënave personale.

Politika zbatohet tek të gjitha llojet e të dhënave, sistemet e informacionit, operacionet dhe proceset brenda mjedisit të Kompanisë që përfshijnë mbledhjen, ruajtjen, përdorimin dhe transmetimin e të dhënave personale. Politika zbatohet për të gjithë punonjësit e kompanisë dhe filialeve të saj në mbarë botën, si dhe për çdo partner biznesi të jashtëm (të tilla si furnizuesit, kontraktorët, shitësit dhe ofruesit e tjerë të shërbimeve) të cilët marrin, dërgojnë, mbledhin, të dhënat në emër të kompanisë.

Faktori i riskut. Mungesa e politikës në fjalë mund të çojë në shkelje jo të qëllimshme të procedurave të kompanisë, zbulimit të paautorizuar të informacionit të klasifikuar të kompanisë ose integritetit të dëmtuar ose dëmtimit të asetit të Kompanisë që çon në humbje të përparësisë konkurruese ose shkeljes së GDPR dhe ligjeve të tjera të zbatueshme, duke shkaktuar humbje financiare dhe/ose ndikim negativ në imazhin e kompanisë.

2. Deklarata e Politikave

CCHBC miraton politikën në fjalë për të siguruar dhe mbajtur pajtueshmërinë me kërkesat ligjore dhe rregullative të zbatueshme për biznesin e saj, në lidhje me mbrojtjen e të dhënave personale. Kompania synon të krijojë një kulturë pozitive të privatësisë ku parimet themelore të privatësisë përfshihen, kuptohen, respektohen dhe përfshihen në veprimtaritë e përditshme të biznesit nga punëtorët e saj:

Ligjshmëria, drejtësia dhe transparenca

Mbani të dhëna personale në mënyrë të drejtë dhe ligjore, duke respektuar të dhënat të drejtën e informimit të subjektit. Përpunoni të dhënat personale vetëm nëse subjekti i të dhënave ka dhënë pëlqimin e tij/saj ose përndryshe nëse përpunimi lejohet me ligj.

Kufizimi i qëllimit

Mblidhni të dhënat personale vetëm për qëllimet e identifikuar në njoftimin përkatës.

Minimizimi i të dhënave

Mblidhni vetëm të dhënat personale që janë të nevojshme për operacionin përkatës të përpunimit.

Saktësia

Mblidhni të dhëna të sakta personale dhe lejoni subjektet e të dhënave që t'i azhurnojnë ato nëse është e nevojshme.

Kufizimi i hapësirës së ruajtjes

Mbani të dhënat personale në një format të identifikueshëm vetëm për intervalin që është i nevojshëm siç identifikohen nga qëllimet e përpunimit për të cilat mblidhen të dhënat.

Integriteti dhe konfidencialiteti

Krijimi i kontrolleve adekuate organizative dhe teknike për të mbrojtur integritetin dhe konfidencialitetin e të dhënave personale, si në formatin digjital dhe ashtu edhe në ate fizik.

Llogaridhënia

Demonstroni përgjegjësi ndaj detyrimeve të GDPR-së duke monitoruar dhe përmirësuar vazhdimisht gjendjen e privatësisë së të dhënave.

3. Pronësia e dokumenteve dhe rishikimi

Pronari i këtij dokumenti është Zyrtari për Mbrojtjen e të Dhënave të Grupit (DPO). Ky dokument duhet të rishikohet dhe nëse kërkohet, përditësohet të paktën një herë në vit.

4. Miratimet

Ky dokument është miratuar nga BSS Data dhe nga Drejtori Analitik

5. Detajet e Politikave

5.1. Ligjshmëria dhe pëlqimi

5.1.1. Njoftim për Privatësi

Çdo aktivitet i përpunimit të të dhënave personale duhet të jetë i ligjshëm. CCHBC duhet të sigurohet që subjekteve të të dhënave, t'u ofrohen informata adekuate në lidhje me përdorimin e të dhënave të tyre personale si dhe të merret pëlqimi i tyre, kur është e nevojshme.

Si rrjedhojë, njoftimi i duhur i privatësisë duhet t'u ofrohet subjekteve të të dhënave në kohën kur mblidhen të dhënat personale, duke përfshirë informacionin e arsyeshëm mbi aktivitetet e përpunimit që do të ndodhin mbi të dhënat e tyre personale, në mënyrë të ligjshme.

Informacioni i mëposhtëm duhet të merret në konsideratë për t'u përfshirë në një njoftim, varësisht nga rrethanat e ndryshme, për të siguruar përpunim të drejtë dhe transparent:

- Detajet e kontaktit për zyrtarin përgjegjës të caktuar për të trajtuar çështjet e mbrojtjes së të dhënave personale
- Detajet e kontaktit të DPO lokale nëse ka
- Qëllimet për të cilat të dhënat personale grumbullohen, përdoren dhe zbulohen
- Baza ligjore për përpunimin e të dhënave personale
- Marrësit e të dhënave personale, nëse ka
- Detajet e çdo transferimi në vendet e treta
- Periudha për të cilën do të ruhen të dhënat personale ose kriteret për përcaktimin e kësaj, sipas qëllimit të biznesit të identifikuar ose sipas mandateve nga rregulloret, cilado që të jetë më vonë.
- Zgjedhjet dhe mjetet që u ofrohen individëve për kufizimin e përdorimit dhe zbulimit të informacionit
- Natyra e detyrueshme ose opcionale e informacionit të kërkuar
- Informata adekuate për të filluar procesin e ushtrimit të drejtave të tyre të privatësisë, siç është qasja në të dhënat e tyre personale

- Se subjektet e të dhënave janë përgjegjëse për të siguruar të dhëna personale të sakta dhe të plota për CCHBC-në dhe si të tillë ata janë përgjegjës për kontaktimin e CCHBC-së nëse kërkohet korrigjimi i një informacioni të tillë

Nëse nevojitet ndonjë qëllim i ri i përpunimit të të dhënave personale, CCHBC duhet të sigurojë njoftimin e duhur të privatësisë subjekteve të të dhënave përpara se informacioni i tillë të përdoret për qëllime që nuk janë komunikuar më parë.

5.1.2. Pëlqimi

CCHBC duhet të marrë pëlqimin e subjekteve të të dhënave në kohën e mbledhjes së të dhënave personale dhe para çdo aktiviteti të përpunimit.

CCHBC duhet të sigurohet se:

- Se pëlqimi kërkohet në mënyrë të kuptueshme, i shkruar në gjuhë të qartë dhe të thjeshtë
- Se pëlqimi është mjaft i dallueshëm nga çështjet tjera me të cilat subjekti i të dhënave ka rënë dakord
- Se pëlqimi është dhënë në mënyrë eksplicite në mënyrë afirmative
- Se pëlqimi është dhënë lirisht nga subjekti i të dhënave
- Sipas paracaktimit, kutitë e zgjedhjes që kërkojnë pëlqimin nuk përzgjidhen
- Ky pëlqim është marrë për secilin qëllim të grumbullimit dhe përpunimit të të dhënave personale
- Është komunikuar qartë dhe intuitive për përdoruesit që ata mund të përditësojnë, menaxhojnë ose tërheqin pëlqimin e tyre në çdo kohë
- Që të dhënat e pëlqimit, duke përfshirë se si dhe kur është dhënë pëlqimi, ruhen automatikisht në një mjedis të sigurt
- Janë regjistruar metadatat përkatëse që lidhen me pëlqimin, siç janë adresa IP, gjeolokacioni, tipi i shfletuesit dhe tipi i pajisjes së bashku me pëlqimin
- Që përdoruesit janë në gjendje të tërheqin pëlqimin e tyre në çdo kohë
- Që kontrollet janë të caktuara për të ndaluar përpunimin e të dhënave personale dhe t'i fshijnë ato kur pëlqimi është tërhequr
- Që proceset e automatizuara janë të caktuara për të marrë pëlqimin e përditësuar nga përdoruesit, pasi proceset e biznesit dhe strategjitë e shfrytëzimit të të dhënave ndryshojnë dhe evoluojnë
- Sistemet e marketingut, shitjeve dhe shërbimeve që përpunojnë të dhënat personale njoftohen për kërkesën për tërheqjen e pëlqimit dhe mund të përgjigjen në kohë reale për të pasqyruar ndryshimet
- Një gjurmë auditimi e pëlqimit menaxhohet në mënyrë të sigurt dhe është lehtësisht e qasshme

5.1.2.1. Pëlqimi I të miturave

CCHCB duhet gjithmonë të sigurohet që pëlqimet për të miturit (nën moshën 16 vjeç) jepen gjithmonë nga përfaqësuesit e të miturve të

mbrojtur dhe në përputhje me parimet e rregullimit të GDPR në mënyrë që procesi të jetë i ligjshëm.

5.1.3. Ligjshmëria në përpunimin e të dhënave personale të ndjeshme

CCHBC duhet të mbledhë, ruaj, përdorë, zbulojë ose të përpunojë 'kategori të veçanta të të dhënave' (p.sh. Informacione në lidhje me origjinën racore apo etnike të një individi, mendime politike, besime fetare ose besime të tjera të një natyre të ngjashme, anëtarësim sindikal, fizik apo mendor shëndetin ose gjendjen ose jetën seksuale siç përcaktohet nga rregullorja e GDPR-së) nëse:

- Individi në fjalë ka dhënë pëlqim të veçantë me shkrim për të përpunuar informacionin
- CCHBC duhet të përpunojë informacionin për të kryer detyrimet sipas ligjit të punës
- CCHBC duhet të përpunojë informacionin për të mbrojtur individin (ose personin tjetër) kur ai individ është fizikisht ose ligjërisht i paaftë për të dhënë pëlqimin e tij
- Përpunimi ndërlidhet me informacionin që është bërë publik nga individi në fjalë ose është i nevojshëm për çështje ligjore.

Përveç kësaj, duhet theksuar se aty ku përpunohen të dhënat personale që kanë të bëjnë me komisionin ose kryerjen e ndonjë vepre penale dhe procedurat e ndërlidhura, CCHBC duhet të sigurojë që bazat për përpunimin e këtij informacioni janë të vendosura, sipas mandatit sipas ligjit vendor, nuk japin një bazë për përpunimin e këtij lloji të të dhënave personale.

5.1.4. Përpunimi automatik i të dhënave personale

Nëse CCHBC përpunon të dhënat personale me mjete të automatizuara pa përdorur ndonjë vendim të marrë nga njeriu, kur kryen ndonjë përpunim të automatizuar plotësisht, CCHBC duhet:

- Të sigurohet se përpunimi është i drejtë dhe transparent duke ofruar informata kuptimplote për logjikën e përfshirë, si dhe rëndësinë dhe pasojat e parashikuara të procesimit
- Të përdorë procedurat përkatëse matematikore ose statistikore për profilizimin (që do të japin një tregues të drejtë në lidhje me atributin që profilizohet)
- Të zbatojë masa të duhura teknike dhe organizative për të mundësuar korrigjimin e pasaktësive dhe minimizimin e rrezikut të gabimeve
- Ruajtja e sigurt dhe qasja në të dhënat personale në një mënyrë që është proporcionale me rrezikun ndaj interesave dhe të drejtave të individit dhe parandalon efektet diskriminuese
- Vendimet e marra nuk duhet të kenë të bëjnë me fëmijët ose të bazohen në të dhëna të ndjeshme personale (përveç nëse në rastin e fundit kontrolluesi i të dhënave ka pëlqim të qartë ose profilizimi është në interesin publik)

Aty ku profilizimi përdoret për të marrë vendime për individët dhe vendimi do të sjellë efekte ligjore (dmth. Krijimi ose mohimi i detyrave ose të drejtave ligjore) për ose përndryshe ka një ndikim të rëndësishëm, individit dhe vendimi bazohen tërësisht në përpunimin e automatizuar, është një vendim i përjashtuar, njerëzit të dhënat e të cilëve përpunohen (p.sh. punëtorët) duhet të jenë në gjendje të:

- Marrin ndërhyrje njerëzore
- Shprehin pikëpamjen e tyre
- Marrin një shpjegim të vendimit dhe t'a sfidojnë atë

5.2. Të drejtat e Subjektit të të dhënave

Të gjithë individët që janë subjekt i të dhënave personale të mbajtura nga CCHBC kanë të drejtë të:

- Kërkojnë informacion dhe/ose qasje në të dhënat e tyre personale
- Kërkojnë fshirje
- Kërkojnë korrigjimin
- Kërkojnë kundërshtim ose kufizim
- Kërkojnë transportueshmëri të të dhënave
- Të jenë pjesë vendimmarrjes së automatizuar

CCHBC duhet të sigurojë një procedurë të përcaktuar mirë për të trajtuar dhe përgjigjur kërkesave të subjektit të të dhënave sipas rregullave të informatave, komunikimit dhe modaliteteve transparente për ushtrimin e të drejtave të subjekteve të të dhënave në kohë dhe në mënyrë efektive.

Regjistrimi i aktiviteteve të përpunimit mund të përdoret për t'u mundësuar palëve të interesuara që të gjejnë informacionin e mbajtur në lidhje me subjektet e të dhënave në departamente, depo ose vende të ndryshme në të gjithë Kompaninë.

CCHBC duhet të caktojë një Zyrtar për Mbrojtjen e të Dhënave dhe organizata përkatëse përgjegjëse për pranimin dhe trajtimin e këtyre kërkesave, ndërsa detajet e duhura të kontaktit duhet të jenë në dispozicion të publikut dhe të sigurohen si pjesë e çdo njoftimi për privatësi, politikën e zbulimit së bashku me të drejtën e subjektit të të dhënave.

5.3. Praktikrat e Sigurisë

5.3.1. Parimet e Përgjithshme

Politika dhe procedurat e sigurisë së informacionit të CCHBC duhet të dokumentohen dhe zbatohen për të siguruar siguri të arsyeshme për të dhënat personale të mbledhura, të ruajtura, të përdorura, të transferuara dhe të deponuara nga CCHBC. Specifikisht:

- Klasifikimi i të dhënave, etiketimi dhe trajtimi i udhëzimeve duhet të vendosen dhe komunikohen

- Duhet të krijohet një procedurë e kontrollit të qasjes, në mënyrë që të ruhet siguria logjike dhe fizike e të dhënave personale
- Duhet të krijohet një politikë e sigurisë fizike për të siguruar mbrojtjen e të dhënave personale nga zbulimi aksidental për shkak të fatkeqësive natyrore dhe rreziqeve mjedisore
- Procedura e shkeljes së të dhënave duhet të krijohet dhe mirëmbahet për t'u marrë me incidentet në lidhje me të dhënat personale ose praktikën e privatësisë. Përgjigjja e menjëhershme pas zbulimit të një shkelje të dhënave që komprometon të dhënat personale së të dhënave, duhet të përputhet me Procedurën e Përgjigjes së Incidentit të Sigurisë së Informacionit.

5.3.2. Politika e Mbrojtjes së të Dhënave Personale

CCHBC duhet të hartojë dhe zhvillojë një politikë të përshtatshme për mbrojtjen e të dhënave personale në mënyrë që të identifikojë në mënyrë adekuate kërkesat minimale të sigurisë dhe kontrollet teknike që ajo ka nevojë për të krijuar. Këto kontrole synojnë të mbrojnë në mënyrë efektive të dhënat personale nga kërcënimet e mundshme, si në formë fizike, ashtu edhe në atë digjitale, si dhe sistemet përkatëse të TI që mbështesin ruajtjen dhe transmetimin e të dhënave personale.

Kërkesat e duhura duhet të njihen për të gjithë ciklin e jetesës së të dhënave personale, nga mbledhja deri në shkarkim. Temat e mëposhtme duhet të mbulohen si pjesë e politikës së mbrojtjes së të dhënave personale:

- Klasifikimi i të dhënave
- Mbledhja e të dhënave
- Kufizimi i përdorimit i të dhënave personale
- Transferimi i të dhënave personale ndërkombëtare
- Ruajtja e të dhënave
- Transmetimi i të dhënave
- Mbajtja e të dhënave
- Shkatërrimi i të dhënave

5.3.3. Privatësia me Dizajn/Automatizëm

Privatësia është një faktor thelbësor në funksionimin normal dhe të qetë të sistemeve dhe aplikimeve të informacionit. CCHBC duhet të sigurojë që privatësia është inkorporuar në çdo projekt që përfshin të dhëna personale, si në kohën e përcaktimit të mjeteve për përpunim ashtu edhe në kohën e përpunimit. CCHBC duhet të sigurojë që privatësia të konsiderohet që nga fillimi dhe nuk është plotësuar ose e shtuar më vonë.

Privatësia me anë të dizajnit do të thotë se çdo projekt që përfshin përdorimin e të dhënave personale të nisura duhet të marrë në konsideratë mbrojtjen e të dhënave nga faza e hershme dhe gjatë tërë ciklit të kohëzgjatjes të projektit. Privatësia me parazgjedhje nënkupton që rregullat më të rrepta të privatësisë zbatohen automatikisht në të gjitha sistemet e informacionit që përmbajnë dhe/ose transmetojnë të dhëna personale

Sa herë që fillon një projekt i ri që përfshin përpunimin e të dhënave personale, CCHBC duhet të:

- Përcaktojë kërkesat që lidhen me përpunimin dhe mjetet e përpunimit në mënyrë që më pas të jenë në gjendje të zbatojnë masat e duhura teknike dhe organizative.
- Vlerësojë nivelin e rrezikut në lidhje me projektin. Përcaktojë nëse projekti është kritik dhe më pas bie nën detyrimin për të kryer një Vlerësim të Ndikimit të Privatësisë së të Dhënave (DPIA). Rrjedhimisht, nëse është e nevojshme, CCHBC duhet të kryejë DPIA dhe të përcaktojë mjetet për të zbutur rreziqet e identifikuar.
- Përcaktojë nëse projekti përfshin shumë rreziqe për të vazhduar dhe në këtë rast të përfundojë projektin.
- Integrojë dhe zbatojë masa të mjaftueshme dhe adekuate për të parandaluar rreziqet.
- Në rast se janë zbatuar masat adekuate dhe projekti plotëson parimet e privatësisë sipas dizajnit dhe atëherë në mënyrë të paracaktuar projekti mund të nënshkruhet.

5.3.4. Vlerësimi i Ndikimit të Privatësisë së të Dhënave (DPIA)

DPIA është një proces për të vlerësuar rreziqet që lidhen me të drejtat dhe liritë e subjekteve të të dhënave dhe rrjedhimisht përcaktojnë masat e duhura për t'i adresuar ato. DPIA përfshin privatësinë me dizajnim në fazat e hershme të projektit dhe gjithashtu mbështesin detyrimin ligjor të CCHBC-së për të demonstruar pajtueshmërinë me GDPR.

CCHBC është e detyruar të kryejë një Vlerësim të Ndikimit të Mbrojtjes së të Dhënave në rastet kur një lloj përpunimi i të dhënave ka të ngjarë të rezultojë në një rrezik maksimal për të drejtat dhe liritë e subjekteve të të dhënave përveç nëse operacioni specifik i përpunimit është përjashtuar në mënyrë eksplicite nga autoriteti mbikëqyrës.

CCHBC duhet të vlerësojë në mënyrë të mjaftueshme rrezikun e lidhur me një proces ose projekt të ri apo ekzistues, me qëllim që të identifikojë efektivisht se cilat operacione të përpunimit duhet të jenë subjekt i DPIA, që mund të rezultojnë në një rrezik të lartë. Në rastet kur kjo nuk është e qartë, një DPIA megjithatë duhet të kryhet. Kriteret e mëposhtme duhet të merren në konsideratë për të identifikuar operacionet e përpunimit që kërkojnë një DPIA për shkak të rrezikut të tyre të brendshëm:

- Evaluimi ose vlerësimi, duke përfshirë profilizimin dhe parashikimin
- Vendimmarrja automatike me ndikim ligjor ose ndikime të ngjashme,

- si përjashtimi ose diskriminimi ndaj individëve
- Monitorimi sistematik, sikur të dhënat e mbledhura përmes rrjeteve ose monitorimi sistematik i zonës me qasje publike
- Kategoritë e veçanta të të dhënave personale (të dhëna të ndjeshme / gjyqësore)
- Të dhënat përpunohen në një shkallë të madhe
- Përputhja ose kombinimi i grupit të të dhënave
- Të dhëna lidhur me të dhënat e grupeve të cenueshme si fëmijët, personat e sëmurë mendërisht etj.
- Përdorimi inovativ ose aplikimi i zgjidhjeve të reja teknologjike ose organizative
- Transferimi i të dhënave përtej kufijve jashtë BE-së
- Parandalimi i subjektit të të dhënave nga ushtrimi i një të drejte ose përdorimi i një shërbimi ose kontrate

Duhet të krijohet një procedurë dhe metodologji e përcaktuar mirë për kryerjen e DPIA-s. Një DPIA mund të kryhet për një operacion të vetëm të përpunimit të të dhënave, si dhe për operacione të shumfishta përpunimi që janë të ngjashme në aspektin e natyrës, fushëveprimit, kontekstit, qëllimit dhe rreziqeve.

Nëse DPIA tregon se përpunimi do të rezultojë në një rrezik maksimal të mbetur, atëherë CCHBC duhet të konsultohet me autoritetin e duhur mbikëqyrës para çdo aktiviteti përpunimi.

Përveç kësaj, në rast se subjektet e të dhënave nuk janë në dijeni të operacionit të ri të përpunimit të veçantë, duhet të krijohet dhe komunikohet një njoftim i duhur për privatësi.

5.3.5. Regjistrimi I Aktiviteteve të Përpunimit (Regjistri i Përdorimit të të Dhënave)

CCHBC duhet të mbajë një regjistër të aktiviteteve të përpunimit nën përgjegjësinë e saj për secilën tërësi Kontrolluesi i të Dhënave në organizatë.

Ky regjistër duhet të përmbajë së paku informacionin e mëposhtëm kur CCHBC vepron si kontrollues i të dhënave:

- Emrin dhe detajet e kontaktit të kontrolluesit dhe, aty ku është e mundur, kontrolluesin e përbashkët, përfaqësuesin e kontrolluesit dhe zyrtarin për mbrojtjen e të dhënave
- Qëllimet e përpunimit
- Një përshkrim të kategorive të subjekteve të të dhënave dhe të kategorive të të dhënave personale
- Kategoritë e marrësve të cilëve u janë zbuluar ose do të zbulohen të dhënat personale, duke përfshirë marrësit në vendet e treta ose organizatat ndërkombëtare
- Kur është e mundur, transferimi i të dhënave personale në një vend të tretë ose një organizatë ndërkombëtare duke përfshirë

identifikimin e atij vendi të tretë dhe dokumentimin e masave të përshtatshme mbrojtëse

- Afatet kohore të parashikuara për fshirjen e kategorive të ndryshme të të dhënave
- Kur është e mundur, një përshkrim i përgjithshëm i masave teknike dhe organizative të sigurisë

Ky regjistër duhet të përmbajë së paku informacionin e mëposhtëm kur CCHBC vepron si përpunues i të dhënave:

- këtu është e aplikueshme, transferimi i të dhënave personale në një vend të tretë ose një organizatë ndërkombëtare duke përfshirë identifikimin e vendit të 3^{të} dhe, dokumentacionin e masave mbrojtëse të përshtatshme
- Kur është e mundur, një përshkrim i përgjithshëm i masave teknike dhe organizative të sigurisë
- Emri dhe detajet e kontaktit të përpunuesit ose përpunuesve dhe çdo kontrollori në emër të të cilit vepron përpunuesi dhe, kur është e mundur, përfaqësuesi i kontrollorit ose përpunuesit dhe zyrtari i mbrojtjes së të dhënave
- Kategoritë e përpunimit të kryera në emër të secilit kontrollues.

Ky regjistër duhet të jetë në dispozicion në çdo kohë, në mënyrë që të sigurohet për autoritetin mbikëqyrës sipas kërkesës, si dëshmi për përmbushjen e kërkesave të GDPR-së.

5.3.6. Kontrollat e Privatësisë

CCHBC duhet të vlerësojë thellësisht kontrollet në vend dhe të caktojë masat minimale teknike dhe organizative në mënyrë që të mbrojnë konfidencialitetin, integritetin, disponueshmërinë dhe përpunimin e ligjshëm të të dhënave personale.

Masat organizative

CCHBC duhet të vazhdojë në zbatimin e masave organizative në mënyrë që të mbrojnë në mënyrë adekuate të dhënat personale në të gjithë mjedisin e korporatës.

Masat indikative organizative në lidhje me pajtueshmërinë e GDPR-së janë renditur më poshtë:

- Menaxhimi i identitetit dhe qasjes - kufizimi i individëve me qasje në të dhënat personale
- Kufizimi në vendet e përpunimit të të dhënave
- Kërkesat e sigurisë fizike në lidhje me të dhënat personale
- Minimizimi i të dhënave personale që mblidhen
- Testimin e rregullt, vlerësimin dhe evaluimin e efektivitetit të masave të sigurisë
- Nismat e ndërgjegjësimit midis punëtorëve që merren me të dhëna personale
- Përfshirja e DPO-së lokale në hartimin e sistemeve dhe proceseve që përfshijnë masat organizative dhe teknike që

kërkohen për të aplikuar mbrojtjen e të dhënave me anë të dizajnit dhe me automatizëm.

Masat Teknike

CCHBC duhet të vazhdojë me zbatimin e masave teknike në mënyrë që të mbrojtë në mënyrë adekuate të dhënat personale në të gjithë infrastrukturën e IT-së.

Masat indikative teknike në lidhje me pajtueshmërinë e DPPM-së janë renditur më poshtë:

- Enkriptimi nga fillimi në fund
- Enkriptimi në gjendje qetësie
- Vlefshmëria e të dhënave
- Autentifikimi
- Autorizimi
- Anonimizimi i të dhënave personale, nëse është e përshtatshme
- Sigurimi i qëndrueshmërisë dhe restaurimit të disponueshmërisë së të dhënave personale, në rast të incidentit të sigurisë (p.sh. rezerva, disponueshmëri e lartë etj.)

5.4. Shkelja e të dhënave personale

Shkelja e të dhënave personale është një incident sigurie që përfshin shkatërrimin, humbjen, ndryshimin, zbulimin e paautorizuar të të dhënave personale të transmetuara, ruajtur ose përpunuar nga CCHBC.

Incidentet e shkeljeve të të dhënave personale mund të ndikojnë negativisht në reputacionin, pajtueshmërinë dhe funksionimin e CCHBC. Aftësia e CCHBC për të identifikuar dhe menaxhuar me shpejtësi incidentet e tilla është kritike për reduktimin e përçarjeve dhe humbjeve.

Si plotësuese e menaxhimit të incidenteve të sigurisë së informacionit, CCHBC, duhet të jetë në gjendje të vlerësojë rrezikun e shkaktuar nga shkelja e të dhënave në lidhje me të drejtat dhe liritë e subjektit të të dhënave kur incidenti përfshin të dhënat personale. Rrjedhimisht, CCHBC duhet të krijojë kanalet e duhura të komunikimit në mënyrë që të njoftojë autoritetin mbikëqyrës dhe/ose subjektin e të dhënave me informacionin e duhur, nëse është e nevojshme.

5.4.1. Vlerësimi i shkeljeve të të dhënave personale

Është shumë e rëndësishme që menjëherë pas marrjes së njoftimit të shkeljes, CCHBC vlerëson rrezikun që mund të rezultojë nga ai, në lidhje me të drejtat dhe liritë e të dhënave.

Gjatë vlerësimit të rrezikut për subjektin e të dhënave si rezultat i një shkeljeje, CCHBC duhet të marrë parasysh rrethanat specifike të shkeljes, duke përfshirë ashpërsinë dhe ndikimin e mundshëm. Vlerësimi duhet të marrë në konsideratë kriteret e mëposhtme:

- Lloji i shkeljes
- Natyra, ndjeshmëria dhe vëllimi i të dhënave personale
- Lehtësia e identifikimit të subjektit të të dhënave

- Ashpërsia e pasojave për subjektin e të dhënave
- Karakteristikat e veçanta të subjektit të të dhënave
- Numri i subjekteve të të dhënave të prekura

5.4.2. Njoftimet

Kur shkelja e të dhënave personale ka të ngjarë të rezultojë në rrezik për të drejtat dhe liritë e personave fizikë, CCHBC duhet të komunikojë shkeljen e të dhënave personale te autoritetit mbikëqyrës, pa vonesa të panevojshme dhe, aty ku është e mundur, brenda 72 orëve pas njoftimit të saj. Kur njoftimi për autoritetin mbikëqyrës nuk bëhet brenda 72 orëve, CCHBC duhet të tregojë arsyet e vonesës.

Kur shkelja e të dhënave personale ka të ngjarë të rezultojë në një rrezik të lartë për të drejtat dhe liritë e personave fizikë, CCHBC duhet të komunikojë shkelje të të dhënave personale subjektit të të dhënave pa vonesa të panevojshme.

Njoftimi për autoritetin mbikëqyrës duhet të përfshijë së paku informacionin e mëposhtëm:

- Përshkrimi i shkeljes
- Detajet e kontaktit
- Natyra e të dhënave të përfshira në shkelje
- Përshkrimi i pasojave të mundshme të shkeljes së të dhënave personale
- Përshkrimi i masave të marra ose të propozuara nga CCHBC për të adresuar shkeljet e të dhënave personale

Njoftimi për subjektin e të dhënave duhet të përfshijë së paku informacionin e mëposhtëm:

- Detajet e kontaktit
- Përshkrimi i pasojave të mundshme të shkeljes së të dhënave personale
- Përshkrimi i masave të marra ose të propozuara nga CCHBC për të adresuar shkeljet e të dhënave personale
- Rekomandime shtesë për subjektet e të dhënave

5.4.3. Regjistri I shkeljeve të të dhënave

Si pjesë e procedurës së menaxhimit të incidentit të sigurisë së informacionit, CCHBC duhet të identifikojë çdo incident të ndodhur, duke përfshirë shkeljet e të dhënave.

Si plotësuese e detajeve të incidentit (data e fillimit, veprimet e ndërmarra, plani i veprimit etj.), Informatat shtesë lidhur me vlerësimin dhe njoftimet duhet të mbahen në mënyrë specifike në rastet e shkeljeve të të dhënave.

5.5. Menaxhimi I përpunuesit të të dhënave

5.5.1. Kërkesat për Diligjencë dhe Kontratat

Në rastet kur CCHBC vepron si një kontrollues i të dhënave dhe shpreh qëllimin e procedimit në një marrëveshje me një palë të tretë të ngarkuar me të dhënat personale që vepron si përpunues i të dhënave, CCHBC duhet të sigurojë që një proces i hollësishëm i përpunuesit të bëhet para se të jepet pëlqimi marrëveshjen përkatëse. Si të tilla, duhet të identifikohen kontrollet e duhura të privatësisë së të dhënave dhe të sigurisë nëse ato duhet të jenë në mjedisin e korporatave të procesorit të të dhënave. CCHBC mban përgjegjësi sipas ligjit në lidhje me atë përpunim.

Përveç kësaj, klauzolat adekuate duhet të përfshihen në të gjitha kontratat për të mbuluar terma të tillë si detyrimet e sigurisë, detyrimet e konfidencialitetit, kërkesat lidhur me sigurimin e integritetit të informacionit si dhe detyrimet lidhur me përdorimin dhe zbulimin e informacionit.

Procesori i të dhënave duhet të nënshkruajë marrëveshjet e mos-zbulimit (NDA) me CCHBC-në për të ndaluar përpunuesin e të dhënave dhe punonjësit e tij nga përdorimi ose zbulimi i informacionit të CCHBC. Kjo duhet të mbulohet si pjesë e kontratës me përpunuesin e të dhënave.

5.5.2. Vlerësoni, Monitoroni dhe Rishikoni Procesorët e të Dhënave

Kur përpunimi duhet të kryhet në emër të CCHBC, duhet të ekzistojë një proces monitorimi dhe auditimi për të vlerësuar se shërbimet e ofruara i përmbahen kërkesave të GDPR-së dhe se përpunuesi i të dhënave i përmbahet të drejtave dhe detyrimeve të parashikuara në kontratat e miratuara.

Monitorimi i raporteve të performancës së përpunuesit së të dhënave dhe dëshmitë përkatëse duhet të merren dhe të rishikohen në një interval të rregullt.

5.6. Përgjegjësia nën GDPR

5.6.1. Bashkëpunimi me Autoritetet Mbikëqyrëse

CCHBC duhet t'i përgjigjet çdo kërkesë për informacion dhe të bashkëpunojë me hetimet nga autoritetet mbikëqyrëse në lidhje me këtë politikë.

5.6.2. GDPR Menaxhimi i Provave

Sipas parimit të llogaridhënies, CCHBC duhet të jetë në gjendje të demonstrojë pajtueshmërinë me kërkesat e mbrojtjes së të dhënave. Dëshmi të tilla duhet të jenë në dispozicion për t'u mbledhur duke regjistruar të gjitha veprimet në përputhje me këtë politikë.

Një listë provave përfshin, por nuk kufizohet në të dhënat e mëposhtme:

- DPIA për proceset e duhura
- Trajnime dhe materiale sensibilizuese në lidhje me privatësinë
- Regjistrimi i aktiviteteve të përpunimit duke përfshirë inventarin e të dhënave personale (regjistri i përdorimit të të dhënave)

- Politika e mbrojtjes së të dhënave dhe procedurat e ndërlidhura
- Të dhënat e kërkesave të subjekteve të të dhënave
- Të dhënat personale shkelin incidentet si pjesë e menaxhimit të incidentit të sigurisë së informacionit
- Njoftime potenciale për subjektet e të dhënave dhe autoritetin mbikëqyrës lidhur me shkeljet e të dhënave

5.7. Trajnimi I privatësisë dhe vetëdijësimi

CCHBC synon të krijojë një kulturë pozitive të privatësisë për njerëzit e saj që është inkorporuar në aktivitetet e përditshme të biznesit. Është e domosdoshme që të gjithë punonjësit të kuptojnë dhe të jenë të vetëdijshëm për përgjegjësitë e tyre, të dinë se si të veprojnë sipas rregullave dhe politikave dhe procedurave organizative, si dhe të jenë në gjendje të identifikojnë ngjarjet eventuale të shkeljeve të të dhënave dhe të jenë plotësisht të vetëdijshëm për kontratën, implikim statutor ose rregullator i çdo shkelje të privatësisë.

Për të arritur këto qëllime, CCHBC duhet të zhvillojë iniciativa vetëdijësuese dhe programet e trajnimit përsëriten të paktën çdo gjorbë të dytë për të rritur vetëdijen e privatësisë midis punonjësve të saj. Trajnimi për vetëdijësimin e privatësisë duhet të dizajnohet me duke pasë në konsideratë këto:

- Sigurimi i informatave, informatave dhe burimeve për punonjësit për t'i mbajtur ata të informuar për kërkesat e tanishme dhe të reja të privatësisë
- Sigurimi i punonjësve me udhëzime adekuate për identifikimin dhe trajtimin e duhur të çështjeve të mbrojtjes së të dhënave që mund të ndikojnë në kryerjen e punës së tyre
- Sensibilizimin e punonjësve për rëndësinë e privatësisë së të dhënave për individët dhe organizatën.
- Duke pranuar se mosrespektimi i rregullave të mbrojtjes së të dhënave, duke përfshirë ato të përcaktuara në këtë politikë, është shkelje e Kodit të Sjelljes së Biznesit të CCHBC-së dhe mund të rezultojë në veprime disiplinore, duke përfshirë shkarkimin.

Iniciativat për ndërgjegjësimin mund të përfshijnë ndër të tjera:

- Materialet
- 'Screensavers'
- Trajnim online
- Prezantime
- Sesionet e takimeve
- Dhurata simbolike

Të gjithë punonjësit që merren me të dhëna personale duhet të marrin pjesë në këto iniciativa ndërgjegjësimi.

5.8. GDPR Monitoring and KPIs

DPO-ja e Grupit është përgjegjëse për kontrollin dhe monitorimin mbi përdorimin e duhur të politikës aktuale, procedurave dhe kontrolleve të lidhura.

Treguesit e performancës së kontrolleve të privatësisë (KPIs) duhet të përcaktohen dhe gjenerohen në baza të rregullta. Paneli përkatës më pas do t'i paraqitet Komitetit përkatës të Privatësisë.

DPO e Grupit duhet të rishikojë periodikisht treguesit e konsideruar në mënyrë që të konfirmojë efektivitetin e kontrolleve në vend. Në rast se vëzhgohen devijime të vazhdueshme negative në lidhje me ekzekutimin e një ose më shumë kontrolleve, DPO-ja e Grupit duhet të sigurojë që të kryhet një analizë e shkakut rrënjësor dhe të përcaktohet dhe të zbatohet një plan veprimi korrektues në kohën e duhur.

KPI-të indikative që i nënshtrohen vlerësimit të mëtejshëm dhe zbatimit të mundshëm:

Kuadri për mbrojtjen e të dhënave personale:

- Përqindja e punonjësve që merren me të dhënat personale, të cilët megjithatë nuk kanë marrë trajnime sensibilizuese lidhur me privatësinë e të dhënave
- Numri i vizitave në një faqe të CCHBC e cila përmban materiale për ndërgjegjësimin e privatësisë
- Përqindja e përpunuesve të të dhënave, për të cilat kontratat e tyre nuk përfshijnë të gjitha klauzolat e kërkuara për privatësi
- Numri i shkeljeve të të dhënave ka ndodhur gjatë muajit të kaluar
- Numri i kërkesës së subjektit të të dhënave të hapur, duke kërkuar të ushtrojë të drejtat e tyre
- Numri i kërkesës së subjektit të të dhënave të mbyllur, duke kërkuar të ushtrojë të drejtat e tyre
- Numri i përjashtimeve ndaj kërkesave për mbajtjen e të dhënave
- Data e fundit e azhurnimit të procesverbalit të procesit dhe të personalitetit inventarit të të dhënave
- Përqindja e procesorit të të dhënave ka marrë pjesë në vlerësimin e privatësisë së procesorit vjetor të të dhënave
- Numri i DPIA-ve që janë kryer

6. Rishikimi i Historisë

Nr i Rishikimit	Data e lëshimit	Autori i Rishikimit	Shënime
Version i 1 ^{te}	Prill 15 2018	Nassos Stylianos (Grupi DPO)	Krijimi
Final	1 Maj	Drejtori i Grupit të të dhënave dhe Analitikës	Finalizimi

7. Annex A - Terms and Definitions

This section provides definitions for terms that are commonly used throughout this Policy.

GDPR	Rregullorja e përgjithshme për mbrojtjen e të dhënave
ZEE	Zona Ekonomike Evropiane
DPO	Zyrtar për Mbrojtjen e të Dhënave
Të dhëna Personale	Çdo informacion që lidhet me një person fizik të identifikuar ose të identifikueshëm ("subjekt i të dhënave"); një person fizik i identifikueshëm është ai që mund të identifikohet, në mënyrë të drejtpërdrejtë ose të tërthortë, në veçanti duke iu referuar një identifikuesi si një emër, një numër identifikimi, të dhëna për vendndodhjen, një identifikues online ose një ose më shumë faktorë specifikë për fizikën, gjenetik, mendor, ekonomik, kulturor ose social të atij personi fizik
Kategoritë e veçanta të të dhënave personale (të dhëna sensitive / gjyqësore)	Të dhënat personale që për nga natyra janë veçanërisht të ndjeshme në lidhje me të drejtat dhe liritë themelore dhe që zbulojnë origjinën racore ose etnike, mendimet politike, besimet fetare ose filozofike, pjesëmarrjen në sindikatë, të dhënat gjenetike dhe biometrike, të dhënat shëndetësore, jetën seksuale, orientimin seksual, bindjet dhe shkeljet
Subjekti i të dhënave	I referohet çdo individ që është subjekt i të dhënave personale të mbajtura nga Kompania, të tilla si punonjësit ose klientët
Pëlqimi	Çdo tregues i dhënë lirisht, specifik, i informuar dhe i qartë i dëshirës së subjektit të të dhënave me anë të të cilit ai, me një deklaratë ose me një veprim të qartë afirmues, nënkupton pëlqimin për përpunimin e të dhënave personale në lidhje me subjektin e të dhënave
Kontrolluesi i të dhënave	Personi fizik ose juridik, autoriteti publik, agjencia ose organi tjetër i cili, i vetëm ose së bashku me të tjerët, përcakton qëllimet dhe mjetet e përpunimit të të dhënave personale; kur qëllimet dhe mjetet e përpunimit të tillë përcaktohen nga ligji i bashkimit ose i shtetit anëtar, kontrolluesi ose kriteret specifike për emërimin e tij mund të sigurohen nga Sindikata ose ligji i Shtetit Anëtar

Përpunues i të dhënave	Një person fizik ose juridik, autoritet publik, agjenci ose një organ tjetër i cili përpunon të dhënat personale në emër të kontrollorit
Pseudo- anonimizimi	Teknika pseudo-anonimizuese përdoren për të zëvendësuar identitetin e një subjekti të të dhënave në mënyrë të tillë që identifikimi të mos jetë direkt i mundur. Megjithatë, duhet të sigurohen informacione shtesë, atëherë subjekti i të dhënave potencialisht mund të ri-identifikohet
Anonimizimi	Të përpunojë një koleksion të të dhënave personale ose informacioneve të tilla që një person fizik nuk mund të identifikohet në bazë të mbledhjes së të dhënave ose informacionit të nxjerrjes
Shkelja e të dhënave personale	Një shkelje e sigurisë që çon në shkatërrimin, humbjen, ndryshimin, zbulimin e paautorizuar të të dhënave personale ose të qasjes në të dhënat personale të transmetuara, të ruajtura ose të përpunuara ndryshe
Palët e Treta	Të gjitha palët e jashtme - duke përfshirë pa kufizim kontraktorët, shitësit, ofruesit e shërbimeve dhe partnerët - të cilët kanë qasje në asetet e informacionit të kompanisë, sistemet e informacionit ose që përpunojnë informacionin e korporatës në emër të Kompanisë

8. Annex B – Subjektet e të dhënave dhe kategoritë e të dhënave personale

CCHBC ka krijuar subjektin e mëposhtëm të të dhënave dhe kategoritë e të dhënave personale:

Kategoritë e subjekteve të të dhënave

- Punëtorët
- Aplikantët e punës
- Individual
- Klientët
- Fëmijët dhe grupet e tjera të prekshme
- Rinia
- Furnizuesit
- Palët e Treta

Kategoritë e të dhënave personale

- **Të dhënat e përgjithshme** personale: çdo informacion që lidhet me një person fizik, të identifikuar ose të identifikueshëm, edhe në mënyrë indirekte duke iu referuar çdo informacioni tjetër, për shembull, emri, mbiemri, adresa e e-mail, qyteti, etj
- **Të Dhënat e Ndjeshme:** të dhënat personale të cilat zbulojnë origjinën racore dhe etnike, besimet fetare, mendimet filozofike ose politike, anëtarësimin në sindikata, gjendjen e shëndetit dhe jetën seksuale
- **Të dhënat gjyqësore:** të dhëna të përshtatshme për zbulimin e sjelljes së paligjshme ose mashtruese, masat gjyqësore ose procedurat gjyqësore dhe masat disiplinore, administrative ose të kontabilitetit ose procedurat
- **Të dhënat biometrike:** të dhënat personale që rezultojnë nga përpunimi teknik specifik që kanë të bëjnë me karakteristikat fizike, fiziologjike ose të sjelljes (që lidhen me natyrën fizike ose trupore dhe përjashton sjelljen për qëllime të marketingut që është kategori më vete më poshtë) e një personi fizik, konfirmojnë identifikimin unik të atij personi fizik, të tilla si imazhet e fytyrës ose të dhënat e gjurmëve të gishtave
- **Të dhënat e sjelljes:** të dhënat e sjelljes janë të gjitha llojet e të dhënave të mbledhura për sjelljen e një individi për qëllime marketingu. Në një kontekst të marketingut dixhital, të dhënat e sjelljes mbledhen kryesisht në internet, por ato gjithashtu mund të vijnë nga burime jashtë linje. Disa lloje të të dhënave të sjelljes janë:
 - Të dhënat e mbledhura për rrjetet e reklamave të sjelljes (shfletimi dhe reagimet ndaj reklamave)
 - Të dhënat e sjelljes të mbledhura në një faqe internet
 - Komentet dhe aktivitetet në faqet e internetit të mediave sociale
- **Të dhënat financiare:** paga, bonus, taksat, pasuritë personale (makina, shtëpia, pajisjet elektronike), detajet bankare, shpenzimet, sigurimet, transaksionet financiare, e.tc.
- **Të tjera**