POLITICA PRIVIND CADRUL GENERAL DE PROTECȚIE A DATELOR CU

CARACTER PERSONAL GROUPE RENAULT ROMANIA

PREAMBUL

Prin Groupe Renault România (denumit în continuare GRR) se înțeleg toate şi oricare din entităţile de naționalitate română afiliate la RENAULT SA Franța, cu sediul în Franța, 92100 Boulogne-Billancourt, Quai Alphonse le Gallo, 13/15, după cum urmează : Automobile Dacia SA, Renault Technologie Roumanie SRL, Renault Mécanique Roumanie SRL şi Renault Commercial Roumanie SRL., Organizaţia Patronală Auto Industrial, Organizaţia Patronală Auto Inginerie Comercială, Federaţia Patronatelor din Industria Auto şi Fundaţia Groupe Renault Romania.

GRR se angajează să păstreze confidenţialitatea datelor personale obținute în cursul activităților sale și să respecte legile și reglementările aplicabile privind prelucrarea acestor date ("Datele cu caracter personal") inclusiv date sensibile ("date sensibile"). Acestea includ, dar nu se limitează la Directiva UE privind protecția datelor 95/46/CE și Regulamentul privind protecția datelor ("GDPR") 2016/679.

GRR a decis să adopte o Politică privind Cadrul General de Protecție a Datelor cu Caracter Personal prin care stabilește măsuri tehnice și organizatorice adecvate de prevenire a procesării neautorizate și ilegale a datelor cu caracter personal și de prevenire a pierderii sau distrugerii accidentale sau a deteriorării acestor date.

Întrebările cu privire la legislația aplicabilă, procedurile care implică colectarea sau utilizarea unor tipuri speciale de date cu caracter personal pot fi adresate **responsabilului pentru protecția datelor** sau DPO, care este responsabil pentru supravegherea respectării acestei **Politici privind Cadrul General de Protecție a Datelor cu Caracter Personal** prin rețeaua de ambasadori pentru protecția datelor, după caz.

GRR își rezervă dreptul de a actualiza **Politica privind Cadrul General de Protecție a Datelor cu Caracter Personal** în orice moment fără notificare prealabilă, pentru a asigura respectarea celor mai adecvate standarde în materie.

ARTICOLUL I - DEFINIȚII

Urmatorii termeni și expresii, atunci când sunt scrise cu majusculă, au următoarele semnificații stabilite mai jos:

„**Grupul de lucru pentru articolul 29**" este alcătuit din reprezentantul autorității de protecție a datelor din fiecare stat membru al UE, al Autorității Europene de supraveghere pentru Protecția Datelor și al Comisiei Europene. Grupul de lucru este independent și acționează în calitate de consultant.

"**Comitetul director al GRR**" este un comitet special dedicat protecției datelor, alcătuit din reprezentanți ai conducerii GRR și DPO.

„**Angajat GRR**" este orice salariat al unei societăți din GRR, inclusiv manageri, manageri de proiect, salariați cu funcții de execuție, stagiari, voluntari, ucenici, precum și colaboratori permanenți sau temporari cu statut de persoană fizică autorizată.

„Operator de date cu caracter personal” = poate fi orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile si structurile teritoriale ale acestora, care stabileste scopul si mijloacele de prelucrare a datelor cu caracter personal sau care este astfel desemnată intr-un act normativ.

„**Ambasador pentru Protecția Datelor**“ sau „APD“ înseamnă persoana din fiecare direcție executivă din cadrul entităților GRR care este responsabilă, sub îndrumarea DPO, pentru asigurarea conformității direcției executive din aria de responsabilitate cu Politica privind Cadrul General de Protecție a Datelor cu Caracter Personal și cu cerințele legale / reglementare aplicabile.

„Persoana imputernicita de operator” = persoana fizica sau juridica, autoritatea publica, agentia sau alt organism care prelucreaza datele cu caracter personal in numele operatorului.

„**Autoritatea pentru Protecția Datelor**" înseamnă Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal – ANSPDCP, autoritatea administrativă responsabilă oficial de protecția datelor cu caracter personal în România. Termenul include orice înlocuitor sau succesor al ANSPDCP.

„**Responsabil de Protecție a Datelor**" sau "**DPO**" înseamnă persoana responsabilă de supravegherea globală a respectării Politicilor de Protecție a Datelor printr-o rețea de Ambasadori pentru Protecția Datelor.

„Date cu caracter personal” = orice informatii privind o persoana fizica identificata sau identificabila *(«persoana vizata») ;* o persoana identificabila este o persoana care poate fi identificata, direct sau indirect, in special prin referire la un element de identificare, cum ar fi nume, un numar de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identitatii sale fizice, fiziologice, genetice, psihice, economice culturale sau sociale.

Prelucrare = orice operatiune sau set de operatiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fara utilizarea de mijloace automatizate, cum ar fi : colectarea, inregistrarea, organizarea, structurarea, stocarea (pastrarea pe orice fel de suport a datelor cu caracter personal), adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispozitie in orice alt mod, alinierea sau combinarea, restrictionarea, stergerea sau distrugerea lor.

"**Jurisdicția reglementată**" înseamnă statele membre ale UE și Spațiul Economic European (SEE). La data intrării în vigoare a prezentei Politici, aceasta include Austria, Belgia, Bulgaria, Cipru, Republica Cehă, Danemarca, Estonia, Finlanda, Franța, Germania, Grecia, Ungaria, Islanda, Irlanda, Italia, Letonia, Liechtenstein, Lituania, Luxembourg, Malta, Olanda, Norvegia, Polonia, Portugalia, România, Slovacia, Slovenia, Spania, Suedia și Regatul Unit. Jurisdicția reglementată include Elveția. Transferurile de date cu caracter personal către Elveția nu necesită autorizarea ANSPDCP.

„**Persoana vizata din punct de vedere al jurisdicției reglementate**" înseamnă orice persoana care era rezident al unei jurisdicții reglementate în momentul colectării datelor sale cu caracter personal.

„**Date cu caracter special**" înseamnă datele menționate la art. 9 din GDPR.

„**Terță parte**" înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal.

ARTICOLUL II - SCOP

Scopul Politicii privind Cadrul General privind Protecția Datelor cu Caracter Personal este de a defini regulile cheie, privind asigurarea celui mai adecvat nivel de protecție datelor cu caracter personal, care sunt aplicabile în cadrul entităților GRR și vizează orientarea entităților GRR în stabilirea programelor de protecție a datelor și respectarea reglementărilor aplicable pentru protecția datelor.

ARTICOLUL III - DOMENIUL DE APLICARE

1. Aria teritorială de aplicare

Prezenta Politica privind Cadrul General de protecție a datelor se aplica Procesării datelor cu caracter personal colectate în România, indiferent dacă prelucrarea are loc în România sau nu.

2. Domeniul de aplicare material

Prezenta politică de protecție a datelor se aplică activităților de prelucrare realizate de către entitățile GRR.

Toate tipurile și categoriile de date cu caracter personal prelucrate de entitățile GRR în cursul activităților lor vor intra în domeniul de aplicare al acestei Politici privind Cadrul General de Protecție a Datelor cu Caracter Personal. Aceste tipuri și categorii includ: Datele personale colectate de la clienți, potențiali clienți, vizitatori, angajați GRR, candidați solicitanți de locuri de muncă, agenți, furnizori și alte părți terțe (enumerarea este doar cu titlu de exemplu).

Politica privind Cadrul General de Protecție a Datelor cu Caracter Personal acoperă atât tipurile automate, cât și cele manuale de procesare.

ARTICOLUL IV - PRINCIPII DE PRELUCRARE

Principii generale

Prelucrarea datelor cu caracter personal sub controlul entităților GRR va fi realizată în conformitate cu legile în vigoare, precum și cu dispozițiile Politicii privind Cadrul General de Protecție a Datelor cu Caracter Personal și, în special, cu respectarea următoarele reguli minime:

• Evaluarea impactului privind protecția datelor, care încorporează principiile "Protecției datelor începând cu momentul proiectării (privacy by design) și în mod implicit (privacy by default)", trebuie să fie efectuată de entitățile GRR pentru orice prelucrare de date.

• Datele personale trebuie obținute în mod echitabil și legal și cu respectarea dreptului de informare al persoanei vizate, cu excepția cazului în care aceasta informare nu este necesară din cauza excepțiilor prevăzute de lege, și trebuie procesată numai dacă persoana vizată și-a dat consimțământul în mod neechivoc sau dacă prelucrarea are alt temei legal.

• Datele personale trebuie colectate numai în scopuri specifice, explicite și legitime și nu trebuie prelucrate într-un mod incompatibil cu acest scop (scopuri). Datele personale vor fi puse la dispoziția părților terte numai în acest scop (scopuri) sau în alte scopuri prevăzute de legile aplicabile.

• Controale adecvate și proceduri tehnice și organizatorice trebuie implementate pentru a asigura securitatea datelor personale și pentru a preveni accesul sau divulgarea neautorizată, potențialele prejudicii care ar putea rezulta din modificarea, distrugerea accidentală sau ilegală sau pierderea accidentală a datelor și împotriva tuturor celorlalte forme ilegale de procesare. Având în vedere obligațiile legale, bunele practici și costurile implementării acestora, măsurile de securitate trebuie să fie concepute astfel încât să asigure un nivel de securitate corespunzător riscurilor reprezentate de procesare și natura datelor cu caracter personal care trebuie protejate.

• Colectarea datelor cu caracter personal trebuie să fie adecvată, relevantă și nu excesivă în raport cu scopul (scopurile) pentru care datele sunt colectate și / sau prelucrate în continuare.

• Datele cu caracter personal nu trebuie păstrate mai mult timp decât este necesar pentru scopul (scopurile) pentru care au fost obținute, cu excepția cazului în care legile aplicabile prevăd altfel.

• Trebuie să se pună în aplicare proceduri pentru a se asigura răspunsuri prompte la întrebările din partea persoanelor vizate, pentru a se asigura că aceștia își pot exercita în mod corespunzător dreptul de acces, de rectificare și de opoziție la prelucrare (cu excepția cazului în care legea aplicabilă prevede altfel).

Datele personale ar trebui prelucrate numai dacă o astfel de prelucrare are temeiuri legitime, incluzând, de exemplu:

• persoana vizată și-a dat în mod clar consimțământul ; sau

• prelucrarea este necesară pentru executarea unui contract in care persoana vizată este parte sau pentru a lua măsuri la cererea persoanei vizate înainte de a încheia un contract ; sau

• procesarea este necesară pentru respectarea unei obligații legale la care este supus operatorul de date; sau

• procesarea este necesară pentru protejarea intereselor vitale ale persoanei vizate ; sau

• procesarea este necesară pentru îndeplinirea unei sarcini de interes public sau în exercițiul autorității publice învestite cu atribuțiile de operator de date; sau

• procesarea este necesară în scopul sau scopurile apărării intereselor legitime urmărite de Operatorul de date sau de terța parte sau părți cărora li se dezvăluie datele cu caracter personal, cu excepția cazului în care aceste scopuri sunt execsive prin raportare la interesele sau de drepturile și libertățile fundamentale ale persoanei vizate.

Datele sensibile

Datele sensibile includ toate datele personale referitoare la :

- Originea rasială sau etnică, opiniile politice sau credințele religioase sau filozofice ale persoanei vizate ;

- Dacă persoana vizată este membră a unui sindicat;

- Sănătatea fizică sau psihică sau starea sau viața sexuală a persoanei vizate ;

- Date biometrice

- Datele specifice considerate sensibile în conformitate cu legislația și reglementările aplicabile;

- Comiterea sau presupusa comitere a unei fapte penale de către persoana vizată; sau - orice procedură pentru o infracțiune comisă sau suspectată a fi fost săvârșită de către persoana vizată, înlăturarea unei astfel de proceduri sau condamnarea pronunțată de orice instanță în astfel de proceduri.

Procesarea datelor sensibile este interzisă cu excepția cazului în care :

1. persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date sensibile, iar acest consimțământ este considerat valabil în conformitate cu legea și reglementările aplicabile ; sau

2. procesarea este necesară pentru scopul (scopurile) îndeplinirii obligațiilor și a drepturilor specifice ale controlorului de date în domeniul dreptului muncii, în măsura în care este autorizată de legea aplicabilă care prevede garanții adecvate ; sau

3. prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale unei alte persoane în cazul în care persoana vizată nu este capabilă din punct de vedere fizic sau legal să-și dea consimțământul ; sau

4. Prelucrarea se efectuează în cadrul unor activități legitime, cu garanții corespunzătoare, de către o fundație, o asociație sau orice alt organism care nu caută un profit cu scop politic, filosofic, religios sau sindical și cu condiția ca procesarea să se refere numai la membrii organismului sau persoane care au contact periodic cu acesta în legătură cu scopul (scopurile) și că datele cu caracter personal nu sunt divulgate unei terțe părți fără consimțământul persoanelor vizate ; sau

5. Prelucrarea se referă la date sensibile care au fost făcute publice de către persoana vizată ; sau

6. Prelucrarea datelor sensibile este necesară pentru stabilirea, exercitarea sau apărarea revendicărilor legale ; sau

7. Prelucrarea datelor sensibile este necesară în scopuri de medicină preventivă, de diagnostic medical, furnizarea de îngrijire sau de tratament sau de gestionare a serviciilor de sănătate și în cazul în care aceste date sensibile sunt prelucrate:

◦ de către un profesionist din domeniul sănătății, în conformitate cu legile sau normele aplicabile de către organismele competente naționale, cu obligația de păstrare a secretului profesional ; sau

◦ de o altă persoană supusă, de asemenea, unei obligații echivalente de secret.

Subcontractarea

Atunci când prelucrarea este efectuată de un subcontractant in numele unei entități GRR, aceasta din urmă alege un subcontractant care să ofere suficiente măsuri tehnice de securitate și măsuri organizatorice pentru a se asigura că procesarea va fi efectuată în conformitate cu Politica privind Cadrul General de Protecție a Datelor cu Caracter Personal iar entitatea GRR trebuie să se asigure că subcontractantul va respecta aceste măsuri. Entitatea GRR care alege subcontractantul se asigură că subcontractantul va fi de acord cu aceste măsuri tehnice de securitate și măsuri organizatorice în scris prin executarea unui contract care prevede în special că subcontractantul va acționa numai conform instrucțiunilor entității GRR.

Transferuri de date în afara jurisdicției reglementate

Entitățile GRR trebuie să se asigure că transferurile de date cu caracter personal în afara UE se bazează pe un mecanism aprobat de autoritatea competentă pentru protecția datelor. În funcție de jurisdicția locală a entității afiliate GRR, aceste mecanisme aprobate pot include:

• utilizarea clauzelor contractuale standard în contractele convenite cu orice furnizor de bunuri sau servicii care primește date personale referitoare la clienții sau angajații unei entități GRR. În acest scop, entitățile GRR pot folosi așa-numitele "clauze model" (oficial "clauze contractuale standard" aprobate de Comisia Europeană pentru transferul de date din UE către țări din afara UE care nu sunt considerate a permite aceeași protecție a datelor cu caracter personal ca legile UE). Aceste clauze pot servi ca punct de referință general pentru transferul de date cu caracter personal din țări cu legi privind protecția datelor care limitează astfel de transferuri;

• utilizarea "regulilor corporative obligatorii" (adică o politică internă de transfer de date care permite entității să transfere date către alte jurisdicții, cu condiția ca acestea să fie aprobate de către Autoritatea competentă pentru protecția datelor). În general, printr-o singură decizie a autorității relevante pentru protecția datelor, entitatea GRR poate evita să solicite o autorizație pentru fiecare transfer în afara jurisdicției sale; și

• utilizarea unui regim de transfer de date, cum ar fi "protecția vietii private" UE-SUA. Având în vedere incertitudinea cu privire la validitatea regimurilor de transfer de date aplicabile (în special pentru transferurile de date din UE către alte jurisdicții), entitățile GRR sunt încurajate să monitorizeze îndeaproape statutul reglementar al regimurilor aplicabile transferurilor de date pe care le efectuează în afara din jurisdicția lor de origine. În cazul invalidării acestor regimuri, entitățile GRR trebuie să poată să se bazeze prompt pe alte mecanisme aprobate, cum ar fi clauzele model și regulile corporative obligatorii.

Ca urmare, nicio Data personală nu poate fi transferată unui importator de date care se afla într-o țară în afara jurisdicției reglementate până cand importatorul de date nu a întreprins următoarele :

- atunci când transferă la o persoană împuternicită de operator, să semneze un acord de prelucrare a datelor, pentru a asigura o protecție adecvată a datelor prelucrate în conformitate cu standardele europene (de exemplu utilizând clauzele aplicabile ale modelului UE propuse de Comisia Europeană sau orice acord care are cel puțin o obligație echivalentă); sau

- să asigure toate celelalte garanții necesare pentru transferul datelor cu caracter personal în conformitate cu legislația aplicabilă (de exemplu clauzele modelului UE).

Responsabilitate

Toate entitățile GRR și direcțiile executive au obligația să demonstreze măsurile pe care le-au luat pentru a asigura conformitatea cu GDPR, precum și pentru a demonstra eficacitatea acestor măsuri ("principiul responsabilității").

ARTICOLUL V - DREPTURILE INDIVIDUALE PRIVIITOARE LA DATELE PERSONALE

Legislația privind protecția datelor prevede că persoanele vizate trebuie să primească informații cu privire la prelucrarea datelor lor personale în momentul colectării datelor. Deși pot exista excepții de la această regulă, acestea sunt rare. Aceste informațiile sunt :

- identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;
- datele de contact ale responsabilului cu protecția datelor;
- scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
- interesele legitime urmărite de operator sau de o parte terță;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- perioada pentru care vor fi stocate datele cu caracter personal sau, daca acest lucru nu este posibil, criteriile utilizate pentru a stabili aceasta perioadă;
- existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
- existenta dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
- dreptul de a depune o plângere în fața unei autorități de supraveghere;
- dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații.

În conformitate cu GDPR, consimțământul expres al persoanei vizate devine regula, inclusiv în ceea ce privește prelucrarea datelor personale fără caracter special.

Consimțământul trebuie să fie dat printr-un răspuns afirmativ clar, care să indice un acord gratuit, specific, informat și lipsit de ambiguitate al persoanei vizate cu privire la prelucrarea datelor cu caracter personal care o privesc, cum ar fi printr-o declarație scrisă, inclusiv prin mijloace electronice sau o declarație orală. În toate cazurile dovada consimțământului trebuie să fie fixată în scopul probațiunii. Tăcerea, « căsuțele » pre-bifate sau inactivitatea nu pot fi luate în considerare drept formă de exprimare a unui consimțământ valabil.

Consimțământul trebuie să acopere toate activitățile de prelucrare a datelor cu caracter personal efectuate în același scop sau scopuri. Atunci când prelucrarea datelor cu caracter personal are scopuri multiple, consimțământul trebuie acordat pentru toate acestea. În cazul în care consimțământul persoanei vizate urmează a fi dat în urma unei cereri prin mijloace electronice, cererea trebuie să fie clară, concisă și să nu perturbe în mod inutil utilizarea serviciului pentru care este furnizat.

În conformitate cu GDPR, în cazul în care operatorul de date cu caracter personal intenționează să prelucreze în continuare datele cu caracter personal într-un alt scop decât cel pentru care au fost colectate, acesta furnizează persoanei respective, înainte de această prelucrare diferită și nouă, informații cu privire la acest nou scop și orice informații suplimentare relevante.

În cazul prelucrării datelor cu caracter personal, persoanele vizate au dreptul, pe baza unei solicitări scrise:

• să obțină o copie a versiunii publice a acestora de la entitațile GRR, la cerere și într-un interval de timp rezonabil;

• să solicite informații despre datele cu caracter personal stocate în legătură cu acestea, inclusiv informații referitoare la modul în care au fost colectate datele cu caracter personal;

• să obțină lista destinatarilor sau categoriilor de destinatari cărora li se transferă datele lor personale;

• să obțină informații cu privire la scopul (scopurile) colectării datelor lor personale și a transferului acestora;

• să rectifice datele personale, atunci când sunt inexacte ;

• să se opună prelucrării datelor lor personale din motive convingătoare și legitime legate de situația lor particulară, cu excepția cazului în care legislația aplicabilă prevede altfel;

• să solicite ștergerea datelor lor personale, dacă acest lucru este posibil din punct de vedere legal și din motive legitime;

• să primească datele personale pe care le-a furnizat entităților GRR, într-un format structurat, utilizat în mod obișnuit și care poate fi citit de o mașină și să aibă dreptul de a transmite aceste date unui alt controlor

ARTICOLUL VI - ACȚIUNI PENTRU IMPLEMENTARE

Program de Training/formare

Entitățile GRR se angajează să implementeze programe de formare privind protecția datelor cu caracter personal pentru angajații GRR implicați în prelucrarea acetor date și să dezvolte instrumentele utilizate pentru prelucrarea datelor cu caracter personal cu privire la principiile conținute în prezenta Politica privind Cadrul General de Protecție a Datelor cu Caracter Personal.

Principiile generale de formare și de sensibilizare vor fi elaborate la nivelul DPO, în timp ce dezvoltarea finală și punerea în aplicare a sesiunilor de formare și de sensibilizare (e-learning, față-în-fata - ...) vor fi efectuate de către fiecare direcție executivă din entitățile GRR, în conformitate cu procesele aplicabile.

Fiecare direcție executivă din entitățile GRR trebuie să definească modul în care efectuează controlul asupra nivelului de formare realizat cu succes. În plus, fiecare direcție executivă din entitățile GRR va determina periodicitatea formărilor recapitulative, instruirea privind protecția datelor cu caracter personal a noilor angajati GRR, ca parte a sesiunii lor de inițiere după integrarea într-o entitate GRR, precum și o formare anuală dedicată în special angajaților GRR care sunt mai implicați în aspectele critice privind datele cu caracter personal.

Direcțiile executive din entitățile GRR pot considera ca următoarele aspecte să fie incluse în programul de instruire : (i) rezumate ale conceptelor cheie; (ii) prezentarea criteriilor pentru prelucrarea legală a datelor cu caracter personal; (iii) rezumate ale motivelor pentru prelucrarea datelor cu caracter personal; (iv) ilustrarea aplicării principiilor cheie în practică; (v) o prezentare generală a politicilor și procedurilor relevante ale entităților GRR ; sau (vi) un studiu de caz interactiv prin care angajații trebuie să gestioneze o problemă de protecție a datelor, cum ar fi solicitarea unei persoane vizate de a accesa toate datele personale referitoare la el sau ea. În toate cazurile, formarea ar trebui să se concentreze asupra cerințelor din cadrul legilor privind protecția datelor aplicabile entităților GRR.

Asigurarea conformității cu regulile GDPR

GRR are:

1. o politică de prelucrare de date cu caracter persoanal aprobată de reprezentantul legal,
2. un ofițer responsabil cu protecția datelor la nivelul GRR (DPO),
3. un Comitet de Coordonare pentru Protectia Datelor (Comitetul director al GRR),
4. o rețea de Ambasadori pentru Protectia Datelor coordonati de către Ofițerul pentru protecția datelor (DPO) la nivelul Grupului.

DPO stabilește politica de protecție a datelor personale de către GRR, în conformitate cu obiectivele strategice ale grupului și se asigură că entitățile GRR aderă la prevederile aplicabile ale regulilor de protecție a datelor și a vieții private.

Direcțiile executive din entitățile GRR își aliniază în mod regulat activitățile la orientările emise de DPO, însă sunt resposabile de modul de exercitare a expertizei în domeniul protecției datelor personale.

DPO trebuie să fie sprijinit în îndeplinirea sarcinilor sale de către o rețea de Ambasadori pentru protecția datelor. DPO trebuie să fie sprijinit de această rețea de ambasadori pentru îndeplinirea sarcinilor sale și trebuie să îi fie furnizate orice alte informații solicitate, integral și fără întârzieri nejustificate.

Rețeaua de ambasadori este ținută de instrucțiunile DPO .

Atribuțiile Ofițerului pentru protecția datelor (DPO):

- informarea și consilierea operatorului, sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului regulament și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;
- monitorizarea respectării prezentului regulament, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului sau ale

persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;

- furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu articolul 35;
- cooperarea cu autoritatea de supraveghere;
- asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la articolul 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

În îndeplinirea sarcinilor sale, responsabilul cu protecția datelor ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.

Monitorizarea internă a activităților de prelucrare

În vederea prevenirii oricăror consecințe grave ale încălcării legilor privind protecția datelor, entitățile GRR implementează programe de conformitate și controale conexe care sunt proiectate în mod rezonabil pentru a preveni, a detecta, a monitoriza și a aborda încălcările potențiale ale legilor privind protecția datelor.

ARTICOLUL VII - PLÂNGERI

Entitățile GRR au un proces intern de soluționare a plângerilor. Persoanele vizate din jurisdicția reglementată pot depune plângere cu privire la orice prelucrare ilegală sau inadecvată a datelor lor personale, care este incompatibilă cu politica de protecție a datelor. Plângerea se depune la:

• responsabilul cu protecția datelor (Data Protection Officer),

• autoritatea relevantă pentru protecția datelor; și

Entitățile GRR vor avea pe site-ul internet instrumente practice care să permită persoanelor vizate să depună plângerile, inclusiv cel puțin una dintre următoarele:

• Adresa de e-mail a responsabilului cu protectia datelor (DPO);

• Adresa poștală.

Cu excepția cazului în care se dovedește deosebit de dificil să se găsească informațiile necesare desfășurării investigației, plângerile trebuie investigate în termen de o (1) lună de la data depunerii.

ARTICOLUL VIII - ASISTENȚA RECIPROCĂ ȘI COOPERAREA CU AUTORITĂȚILE DE PROTECȚIE A DATELOR

Entitățile GRR vor coopera cu Autoritatea pentru Protecția Datelor cu privire la orice aspecte legate de protecția datelor, astfel:

- prin punerea la dispoziție a personalului necesar pentru dialogul cu autoritățile de protecție a datelor,
- prin revizuirea activă, luând în considerare orice decizii luate de autoritățile de protecție a datelor și opiniile Grupului de lucru pentru articolul 29,
- răspunzând cererilor de informații sau plângerilor din partea autorităților de protecție a datelor
- prin aplicarea recomandărilor sau sfaturilor relevante din partea autorităților lor competente pentru protecția datelor.

Dacă Autoritatea pentru Protecția Datelor solicită informații sau își exercită în alt mod dreptul de investigație, DPO trebuie informat fără întârziere de către rețeaua de Ambasadori pentru protecția datelor. În acest caz, DPO va acționa în calitate de coordonator pentru a formula un răspuns adecvat la solicitare, după consultarea cu rețeaua de ambasadori pentru protecția datelor, după caz, precum și cu alți responsabili și / sau corespondenți (de exemplu: avocat, consilier juridic, ofițer de etică și conformitate și / sau resposabil securitate IT).

În plus, DPO va acționa ca prim și direct contact cu respectivele Autoritatea pentru Protecția Datelor.

ARTICOLUL IX - DATA INTRĂRII ÎN VIGOARE ȘI TERMENUL

Politica privind Cadrul General de protecție a datelor va intra în vigoare la **25 mai 2018** pentru o perioadă nedeterminată.

ARTICOLUL X - IMPLEMENTARE - NOTIFICAREA BREȘELOR DE SECURITATE - REVIZUIRE - RAPORTARE

Punerea în aplicare

Fiecare direcție executivă din entitățile GRR este responsabilă pentru asigurarea unui program adecvat și eficient de protecție a datelor. Pentru a facilita buna funcționare a acestor programe, GRR va supraveghea implementarea și funcționarea continuă a programelor de conformitate a entităților GRR pentru protecția datelor. Programele de conformitate pentru protecția datelor ale entităților GRR vor face obiectul unor audituri interne periodice care vor testa eficacitatea controalelor de conformitate a protecției datelor.

Notificare privind încălcarea normelor de protectie a datelor cu caracter personal

Când datele cu caracter personal sunt susceptibile de a fi afectate de o breșă de scuritate, Ambasadorul din direcția executivă în cauză trebuie imediat să notifice DPO. Apoi, entitatea GRR din care face parte direcția executivă în cauză, împreună cu DPO, trebuie să notifice Autoritatea de Protecție a datelor, fără întârzieri nejustificate și, acolo unde este posibil, în termen de 72 de ore de la momentul in care entitatea GRR devine conștientă de încălcarea securității datelor cu caracter personal, în activitatea direcției executive în cauză.

Entitatea GRR (entitățile) care ar putea acționa în calitate de Operator de date cu caracter personal trebuie să notifice entitățile afiliate care ar putea acționa în calitate de împuterniți ai

operatorului de date cu caracter personal, fără intarzieri nejustificate, după ce au luat cunoștință de breșa de securitate.

Rețeaua de ambasadori pentru protecția datelor documentează orice breșă de securitate, , efectele sale și măsurile de remediere luate pentru a informa printr-un raport în acest sens DPO. Această documentație trebuie să permită DPO să verifice respectarea cerințelor legate de Notificarea unui breșe de securitate Autorității de supraveghere pentru protecția datelor.

Daca breșa de securitate este de natură să conducă la un grad ridicat de risc pentru drepturile și libertățile persoanelor vizate, entitatea GRR în cauză trebuie să notifice, de asemenea, persoanele vizate afectate de breșă, fără întârzieri nejustificate, cu excepția cazului în care se aplică anumite excepții (de exemplu, compania GRR a luat măsuri pentru a reduce riscul pentru persoanele vizate și / sau notificarea ar implica eforturi disproporționate și / sau persoanele vizate au fost informate prin intermediul comunicărilor publice).

Revizuire

DPO va asigura revizuirea și actualizarea periodică a Politicii privind Cadrul General de Protecție a Datelor cu Caracter Personal, de exemplu ca o consecință a unor schimbări majore în structura corporativă și în mediul de reglementare.

În această privință, DPO va ajuta la definirea și actualizarea măsurilor organizatorice și tehnice care urmează să fie puse în aplicare atunci când se colectează, prelucrează, și / sau utilizează date cu caracter personal în conformitate cu cerințele legale. Astfel de măsuri organizatorice și / sau tehnice pot intra în vigoare imediat după ce DPO a revizuit și aprobat compatibilitatea acestora cu această Politică privind Cadrul General de Protecție a Datelor cu Caracter Personal.

Raportarea

Entitățile GRR raportează informații privind încălcările securității datelor, orice audit sau examinare de către Autoritatea pentru Protecția Datelor sau orice comunicare cu Autoritatea pentru Protecția Datelor către GRR.