Principis generals de la Política corporativa de privacitat i protecció de dades

29 de gener de 2025

Control de versions

Versió	Data	Control
1	28/03/2022	Revisió i actualització dels Principis generals de la Política.
2	29/01/2025	Revisió i actualització dels Principis generals de la Política.

Contingut

1. Introducció

1.1 Antecedents

CaixaBank, S.A. és una entitat de crèdit, capçalera d'un grup que presta serveis financers i d'inversió (d'ara endavant, "CaixaBank" o l'"Entitat"). Com a tal, es regeix pels estàndards més elevats de respecte al dret fonamental de protecció de dades de caràcter personal, així com a la preservació de la confidencialitat de la informació que tracta. Aquests constitueixen pilars fonamentals sobre els quals s'assenta la confiança, valor essencial de la seva activitat.

En aquest context, el Consell d'Administració de CaixaBank, coincidint amb l'inici de l'aplicació el 25 de maig del 2018 del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril del 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (d'ara endavant, el "Reglament general de protecció de dades" o l'"RGPD"), va fer un pas més en el seu compromís amb la confidencialitat i amb la protecció de les dades personals establint, mitjançant la Política a què fan referència aquests principis (d'ara endavant, la "Política"), un marc general de gestió de la privacitat i la protecció de dades a l'Entitat. La Política està adaptada a les noves disposicions normatives i va formalitzar l'adopció i el seguiment dels principis que la norma esmentada incorpora, com ara la privacitat per defecte i per disseny, l'enfocament de riscos i la responsabilitat proactiva.

Així mateix, l'abril del 2019 la Comissió Europea va publicar les Directrius ètiques per a una intel·ligència artificial fiable, que constitueixen el primer marc europeu per aconseguir l'ús a la Unió d'una intel·ligència artificial licita, ètica i robusta. Seguidament, el febrer de 2020 es va publicar el Llibre blanc sobre intel·ligència artificial: "Un enfocament europeu orientat a l'excel·lència i la confiança", que planteja la necessitat d'establir un marc regulador de l'ètica en l'ús de les dades i els sistemes d'intel·ligència artificial.

Fruit de tot això, la Comissió Europea, l'abril del 2021, va publicar la seva primera proposta de text per al que serà el futur Reglament europeu, mitjançant el qual es pretenen establir normes harmonitzades en matèria d'intel·ligència artificial (llei d'intel·ligència artificial).

Aquesta proposta va anar seguida de la posició adoptada pel Consell de la Unió Europea, el desembre de 2022, sobre el Reglament d'Intel·ligència Artificial, encaminat a garantir que els sistemes d'intel·ligència artificial (IA) introduïts al mercat de la UE i utilitzats a la Unió siguin segurs i respectin la legislació vigent en matèria de drets fonamentals, així com els valors de la Unió.

El 9 de desembre de 2023 el Consell de la Unió Europea, liderat per la presidència espanyola, i el Parlament Europeu van arribar a un acord provisional per a l'aprovació definitiva del futur Reglament pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial (Reglament d'Intel·ligència Artificial o *AI Act*).

Fruit de tot això, el 21 de maig de 2024, el Consell de la Unió Europea va donar la seva aprovació final al Reglament pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial (Reglament de IA) i finalment, el dia 12 de juliol de 2024, es va publicar al Diari Oficial de la Unió Europea (DOUE). A partir d'aquesta publicació, el Reglament va entrar en vigor el dia 2 d'agost de 2024, sent directament aplicable en tots els Estats membres, sense necessitat de transposició a lleis nacionals. La regla general és que serà

aplicable als 24 mesos des de l'entrada en vigor (a partir del 2 d'agost de 2026) amb excepcions per a certes disposicions específiques: i) les prohibicions de sistemes d'IA que plantegin riscos inacceptables (pràctiques d'IA prohibides) entraran en vigor al cap de 6 mesos (2 de febrer de 2025); ii) les normes de governança i les obligacions per als models d'IA d'ús general que hagin de complir requisits de transparència seran aplicables al cap de 12 mesos (2 d'agost de 2025); iii) als 24 mesos s'aplicaran la resta de disposicions (sistema de gestió de riscos, de qualitat, etc.), i iv) als 36 mesos s'aplicaran les regles de classificació dels sistemes d'IA d'alt risc —components de seguretat d'un producte— (2 d'agost de 2027).

Així mateix, el dia 5 de setembre de 2024, la Comissió va signar, en nom de la Unió Europea, el Conveni Marc del Consell d'Europa sobre Intel·ligència Artificial i Drets Humans, Democràcia i Estat de Dret. És el primer tractat internacional legalment vinculant destinat a garantir que l'ús dels sistemes d'intel·ligència artificial sigui totalment coherent amb els drets humans, la democràcia i l'Estat de dret. En aquest sentit, proporciona un marc legal que comprèn el cicle de vida complet dels sistemes d'IA, promou el progrés i la innovació en IA, i a la vegada gestiona els riscos que pot plantejar per als drets humans, la democràcia i l'Estat de dret.

Per part seva, l'Agència Espanyola de Protecció de dades va publicar dos guies sobre intel·ligència Artificial, la Guia sobre Adequació a l'RGPD de tractaments que incorporen Intel·ligència Artificial. Una introducció, el febrer de 2020 i de Requisits per a Auditories de tractaments que incloguin IA, el gener de 2021.

El Consell d'Administració de CaixaBank, mitjançant la Política a la qual es refereixen aquests principis, pretén establir els principis que l'Entitat i el seu Grup apliquen en el tractament de la informació personal, els drets que reconeix als interessats i el marc de govern intern de què, en matèria de privacitat, volen dotar-se. A la Política es regula també la figura del delegat de protecció de dades.

Finalment, el Consell d'Administració, amb la Política a què fan referència aquests principis, pretén garantir l'establiment dels procediments i les mesures necessaris per assegurar una gestió del risc de la privacitat d'acord amb l'apetit al risc de l'Entitat i el Grup.

El Consell d'Administració té la facultat indelegable per a la determinació de les polítiques i estratègies de l'Entitat d'acord amb l'article 249 bis del text refós de la Llei de societats de capital.

1.2 Risc de protecció de dades i confidencialitat de la informació.

L'article 8 de la Carta dels Drets Fonamentals de la Unió Europea estableix el dret de qualsevol persona a la protecció de les dades de caràcter personal que li concerneixin, concretant que les dades hauran de ser tractades de manera lleial i per a fins concrets. En aquest sentit, l'RGPD és el marc de què s'ha dotat la Unió Europa per garantir aquest dret fonamental i la seva no afectació establint les regles que han de regir els tractaments de dades. La Política a què es refereixen aquests principis cobreix el risc de CaixaBank d'afectar aquest dret fonamental quan en els seus processos tracta dades personals.

Així mateix, la Política a què es refereixen aquests principis cobreix el risc de secret bancari establert a l'art. 83 de la Llei 10/2014, de 26 de juny, d'ordenació, supervisió i solvència d'entitats de crèdit consistent en el deure de reserva de la informació a què estan obligades les entitats de crèdit en relació amb les informacions relatives als saldos, posicions, transaccions i altres operacions dels seus clients.

Finalment, i derivat dels anteriors, el risc objecte de gestió i control per la Política a què es refereixen aquests principis és el risc de protecció de dades i privacitat, establert al segon nivell dins el Catàleg Corporatiu de Riscos, com a component del risc legal i regulatori, i definit com el risc relacionat amb

l'incompliment de la normativa relacionada amb la protecció de dades de caràcter personal i la privacitat de les persones,

Derivat d'aquesta configuració, el risc de protecció de dades i privacitat està estretament relacionat amb altres riscos corporatius com el risc tecnològic, i més concretament amb el risc de seguretat de la informació.

1.3 Objectiu

La Política a què fan referència aquests principis té com a objectius:

- Transmetre a tots els empleats i les empleades, els directius i els membres de l'òrgan d'administració de l'Entitat i del Grup CaixaBank el missatge que el Grup vetlla perquè la seva activitat estigui basada en el respecte a les lleis i a les normes vigents a cada moment, així com en la promoció i defensa dels valors corporatius i principis d'actuació establerts al seu Codi ètic i, per consegüent, enllaça amb els seus valors ètics, ratificant la voluntat ferma de mantenir una conducta de compliment estricte en matèria de privacitat i ús ètic de les dades i els components d'intel·ligència artificial.
- Establir un marc general per a la gestió de la privacitat i la protecció de dades de caràcter personal, i l'ús ètic de les dades i els components d'intel·ligència artificial, adaptant-lo a les noves disposicions normatives. El marc comprendrà el conjunt de mesures dirigides a la prevenció, detecció i reacció i identificarà els riscos de privacitat i controls associats a aquests que s'estableixin.
- Assegurar davant els accionistes, clients, proveïdors, organismes supervisors i la societat en general que l'Entitat i el seu Grup compleixen els deures de supervisió i control de la seva activitat pel que fa a la privacitat i l'ús ètic de les dades i els components d'intel·ligència artificial, establint mesures adequades per prevenir o reduir el risc d'actuacions no respectuoses amb la normativa vigent, i que, per tant, s'exerceix el degut control legalment procedent sobre administradors, directius, empleats i altres persones associades.

El contingut de la Política a què fan referència aquests principis inclou:

- Estratègia o principis generals que regeixen la gestió de la privacitat i la protecció de dades
- Marc de govern.
- Aspectes generals de la gestió en matèria de privacitat, protecció de dades i ús ètic de les dades i els components d'intel·ligència artificial:
    - Delegat de protecció de dades (d'ara endavant, DPO) i altres figures responsables
    - Tractaments i legitimació
    - Drets dels interessats
    - Avaluacions d'impacte
    - Mesures tècniques
    - Proveïdors
    - Comunicació i formació
- Marc de control
- Marc d'informació

2. Àmbit d'aplicació

La Política a què fan referència aquests principis té caràcter corporatiu. En conseqüència, els principis d'actuació definits són aplicables a totes les societats del Grup CaixaBank amb exposició al risc de protecció de dades i a l'ús ètic de les dades i els components d'intel·ligència artificial. Els òrgans de govern d'aquestes societats adoptaran les decisions escaients per tal d'integrar les disposicions d'aquesta Política, tot adaptant, seguint el principi de proporcionalitat, el marc de govern a la idiosincràsia de la seva estructura d'òrgans de govern, comitès i departaments, i els seus principis d'actuació, metodologies i processos a allò que descriu aquest document.

Aquesta integració podrà suposar, entre altres decisions, l'aprovació d'una política pròpia per part de la filial. L'aprovació serà necessària en aquelles societats del grup que precisin adaptar el que disposa la Política a què fan referència aquests principis a les seves especificitats pròpies, ja sigui per matèria, per jurisdicció o per rellevància del risc a la filial. En aquells casos en què les activitats de control i gestió del risc de la filial es facin directament des de CaixaBank, ja sigui per materialitat del risc a la filial, per raons d'eficiència o perquè la filial hagi externalitzat a CaixaBank la gestió operativa d'aquest risc, els òrgans de govern de les societats del Grup afectades almenys prendran coneixement de l'existència d'aquesta Política corporativa i de la seva aplicació a les societats del Grup esmentades. L'adhesió a aquesta Política corporativa per part dels òrgans de govern de les societats del Grup es realitzarà quan, sent aplicables els principis d'actuació de la Política corporativa, la filial no elabori una política pròpia i el contingut de la Política corporativa estableixi principis, obligacions i activitats que la societat del Grup ha de seguir i realitzar directament.

En qualsevol cas, la Direcció de *Compliance* de CaixaBank, atès el seu caràcter corporatiu, vetllarà perquè la integració d'aquesta Política a les societats del Grup sigui proporcionada, perquè, en cas que les societats del Grup aprovin polítiques pròpies, estiguin alineades amb la política corporativa, i per la consistència a tot el Grup CaixaBank.

Finalment, la Política a què fan referència aquests principis, a més de ser corporativa, té la consideració de política individual de CaixaBank, matriu del Grup CaixaBank.

La Política a què es refereixen aquests principis és directament aplicable als empleats, directius i membres de l'òrgan d'administració de l'Entitat en relació amb el marc de govern dels tractaments de dades que es fan amb persones físiques (clients potencials, accionistes, empleats, representants i apoderats de persones jurídiques com ara proveïdors o *partners)*

3. Marc normatiu. Normativa i estàndards d'aplicació

La Política a què fan referència aquests principis es regirà pel que preveu la normativa aplicable vigent, així com per aquella que la modifiqui o substitueixi en el futur. En concret, en la data de l'elaboració de la Política, la normativa vigent aplicable a la matriu del Grup és la següent:

- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril del 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades).
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
- Llei 11/2022, de 28 de juny, General de Telecomunicacions.
- Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.
- Reglament (UE) 2023/2854, Llei de dades
- Reglament (UE) 2022/868, Llei de governança de dades
- Reglament (UE) 2022/2065, Llei de serveis digitals
- Llei 10/2014, de 26 de juny, d'ordenació, supervisió i solvència d'entitats de crèdit, en relació amb el que preveu el seu article 83, Obligació de secret.
- Reglament (UE) 2024/1689 del Parlament Europeu i del Consell, de 13 de juny de 2024 pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial d'acord amb el que s'estableix al considerant 9 i 10 d'aquest, així com al seu art. 27. Guies dels supervisors nacionals i europeus (AEPD i EDPB).

En el cas de les societats del Grup o, si escau, sucursals subjectes a jurisdiccions estrangeres o normativa sectorial complementària, les polítiques i els procediments que aquestes societats del Grup o sucursals desenvolupin tindran en compte, a més de la seva normativa pròpia, les obligacions contingudes a la normativa assenyalada anteriorment mentre no siguin contradictòries amb els requisits específics de la jurisdicció o la normativa sectorial corresponent.

Finalment, a cadascuna de les societats o, si escau, sucursals del Grup es desenvoluparan els marcs, les normes, les guies o els procediments que siguin necessaris per a la implementació, l'execució i el compliment correctes de la Política a què fan referència aquests principis.

4. Principis generals de la gestió del risc de privacitat i protecció de dades

Els principis que orientaran la presa de decisions del Grup CaixaBank en matèria de privacitat i protecció de dades són els següents:

- **Tractament de les dades de manera lícita, lleial i transparent**. Es respectarà l'ordenament jurídic aplicable, el tractament de les dades personals es farà sempre a l'empara d'alguna de les condicions legals que el permeten i s'informarà l'interessat sobre aquesta qüestió incloent-hi, si escau, informació sobre l'elaboració de perfils i les seves conseqüències.
- **Tractament de les dades per a fins determinats, explícits i legítims.** No es tractarà la informació per a fins incompatibles amb aquells dels quals s'hagi informat l'interessat.
- **Tractament únicament de les dades adequades, pertinents i limitades** a cada finalitat del tractament.
- **Tractament de dades exactes i actualitzades**. S'adoptaran les mesures que permeten suprimir o modificar la informació, de manera que es mantingui exacta i al dia.
- **Conservació de les dades únicament durant el temps necessari**. En la majoria dels casos, les dades deixen de ser necessàries quan finalitza la relació contractual o de negoci (o quan es retira el consentiment per utilitzar-les). A partir d'aquest moment, es procedirà a l'adaptació i la modificació dels tractaments de dades corresponents adequant-los, si escau, al nou títol habilitador (com ara el compliment d'obligacions legals o la formulació, l'exercici o la defensa dels seus drets i interessos) i, finalment, se suprimiran.
- **Tractament de dades amb mesures de seguretat de la informació.** CaixaBank assegura l'adequada protecció de les dades personals i de la informació, desplegant mesures de seguretat per protegir-se adequadament contra amenaces i riscos que poguessin afectar la confidencialitat, integritat i disponibilitat dels seus sistemes, actius d'informació o recursos.
- **Actuació amb responsabilitat proactiva**. CaixaBank es dotarà dels procediments i eines necessaris per documentar i conservar totes les accions que duguin a terme, de conformitat amb la Política i la normativa de protecció de dades, en relació amb els tractaments que fan, amb la finalitat no només de complir proactivament amb la normativa vigent, sinó també per estar, en qualsevol moment, en disposició d'acreditar el seu compliment.
- **Privacitat des del disseny i per defecte**. CaixaBank disposa de mesures tècniques i organitzatives durant tot el cicle de vida del tractament d'acord amb els riscos per als drets i llibertats d'aquest i tenint en compte la naturalesa, l'àmbit, el context i les finalitats del tractament.

5. Marc de govern.

Els pilars sobre els quals s'assenta el marc de govern del risc de protecció de dades i privacitat al Grup CaixaBank són:

- Compliment dels principis recollits a la Política a què fan referència aquests principis per part de les societats del Grup dins el seu àmbit d'aplicació.
- Supervisió corporativa de l'entitat matriu.
- Alineació d'estratègies entre les societats del Grup i, al seu torn, alineació amb les millors pràctiques, amb les expectatives supervisores i amb la regulació vigent.
- Implicació màxima dels òrgans de govern i direcció de les societats del Grup.
- Marc de control intern basat en el model de Tres Línies de Defensa, que garanteix la segregació estricta de funcions i l'existència de diverses capes de control independent.

6. Marc de gestió per a la privacitat i la protecció de dades

6.1. Delegat de protecció de dades (DPO)

És l'assessor i supervisor del compliment de la normativa sobre privacitat. Depèn funcionalment del DPO corporatiu, al qual reporta i amb el qual es coordina. Les seves responsabilitats, obligacions i pautes de funcionament es detallen a continuació.

6.1.1 Nomenament

És responsabilitat del Comitè de Direcció de l'Entitat el nomenament del delegat de protecció de dades, així com el seguiment de la seva execució. Es nomenarà el delegat de protecció de dades:

- Tenint en compte les seves qualitats professionals i, en particular, els seus coneixements especialitzats en dret, la pràctica en matèria de protecció de dades i la seva capacitat per desenvolupar les funcions que se li assignen.
- Amb vocació de grup, per la qual cosa les societats del Grup establertes a Espanya que adoptin aquesta Política a què fan referència aquests principis com a pròpia hauran de nomenar com a delegat de protecció de dades al delegat de protecció de dades de CaixaBank.
- Amb caràcter corporatiu, ja que el delegat de protecció de dades de CaixaBank serà el delegat corporatiu de protecció de dades, del qual dependran funcionalment els delegats de dades de les empreses del perímetre i els que poguessin nomenar-se en altres jurisdiccions diferents de l'espanyola.

El nomenament del delegat de protecció de dades es publicarà i es comunicarà a l'autoritat de control.

6.1.2 Encaix organitzatiu i funcions

L'Entitat garantirà, en tot moment, que el delegat de protecció de dades:

- Participa de manera adequada i en temps adient en totes les qüestions de protecció de dades.

- Disposa dels recursos necessaris per a l'exercici de les seves funcions i el manteniment dels seus coneixements especialitzats, i rep formació adequada.
- Té accés a les dades personals i operacions objecte de tractament.
- Ret comptes directament al nivell jeràrquic més alt.
- Gaudeix d'independència en l'exercici de les seves funcions en els termes previstos a l'apartat 6.1.4 de la Política a què fan referència aquests principis.

El delegat de protecció de dades desenvoluparà, com a mínim, les funcions següents:

- Assessorar, informar i supervisar sobre el compliment en les àrees/matèries següents:
    - Aplicació dels principis relatius al tractament de les dades personals.
    - Identificació i aplicació de les bases jurídiques del tractament.
    - Compatibilitat de finalitats diferents de les que van originar la recollida de les dades.
    - Normativa sectorial que pugui afectar el tractament de les dades personals.
    - Informació als afectats.
    - Exercici de drets dels interessats.
    - Contractació d'encarregats.
    - Transferències internacionals de dades.
    - Política de protecció de dades.
    - Conscienciació dels empleats i l'organització.
    - Formació als empleats.
    - Auditoria de protecció de dades.
    - Registres d'activitats de tractament.
    - Protecció de dades des del disseny.
    - Anàlisi de risc dels tractaments.
    - Mesures de seguretat adequades.
    - Violacions de seguretat.
    - Si escau, garanties per al responsable.
- Actuar com a mediador entre els clients i l'Entitat en les reclamacions sobre protecció de dades.
- Cooperar i actuar com a punt de contacte entre l'Entitat i l'AEPD o una altra autoritat de control, per a qüestions relatives al tractament, i fer consultes sobre qualsevol altre assumpte.
- Actuar com a punt de contacte per als interessats i en l'exercici de drets per part seva.

El delegat de protecció de dades desenvoluparà les seves funcions prestant l'atenció deguda als riscos associats a les operacions de tractament i tenint en compte la naturalesa, l'abast, el context i les finalitats del tractament.

Les funcions anteriors que, segons el que estableix la Política de Control Intern, estiguin atribuïdes a les àrees de Compliment i Auditoria Interna, seran desenvolupades de manera directa i autònoma per aquestes unitats, amb la coordinació establerta a l'apartat 6.1.10.

6.1.3 Facultats

En el desenvolupament de les seves funcions, el delegat de protecció de dades té atribuïdes les facultats següents:

- Accedir a la informació i a les dades personals dels interessats.
- Accedir a les operacions del tractament automatitzades i no automatitzades.
- Consultar documentació, sistemes, programes, bases de dades i, en general, qualsevol suport relatiu a les dades personals o al seu tractament.
- Participar en reunions en què es tractin qüestions relatives als tractaments de dades personals.
- Mantenir la interlocució amb l'AEPD i amb altres autoritats de control.
- Tenir accés directe i reportar periòdicament a l'alta direcció, a través del Comitè de Privacitat i de manera directa.
- Organitzar internament els seus recursos.

6.1.4 Independència

L'Entitat no impartirà instruccions, sancionarà ni destituirà el DPO per l'exercici de les seves funcions. L'anterior s'entén sens perjudici de la facultat organitzativa que l'assisteix.

El delegat de protecció de dades té accés i ret comptes al nivell jeràrquic més alt.

6.1.5 Disponibilitat i participació efectiva

L'Entitat s'assegurarà que el DPO està disponible per a les seves funcions internes i externes, i participa efectivament en les anàlisis i valoracions sobre tractaments de dades personals.

6.1.6 Dotació de mitjans

El delegat de protecció de dades, en el desenvolupament de les seves funcions, disposarà dels mitjans organitzatius necessaris per desenvolupar la seva activitat i comptarà amb el suport intern legal, regulador i tècnic de l'Entitat per fer-ho. També podrà recórrer a la contractació d'assessors externs per a aquells temes que, al seu parer, resultin necessaris.

Per al desenvolupament correcte de les seves atribucions, el DPO haurà de comptar amb mitjans adequats, almenys, per desenvolupar les funcions bàsiques següents:

- Assessorar i donar suport a l'Entitat mitjançant l'actualització de la normativa aplicable en matèria protecció de dades i en la detecció de possibles situacions de risc de compliment.
- Assessorar i prestar assistència a l'Entitat mitjançant la interpretació de normes i aportant coneixement i anàlisis de la normativa vigent i dels projectes normatius en curs per tal de preveure el seu impacte en l'Entitat.
- Assessorar en la supervisió i, en particular, en el disseny de controls de primer nivell.
- Assessorar i donar suport en la formació dels empleats en matèria de protecció de dades.
- Assessorar i donar suport a la tercera línia de defensa en la realització de controls periòdics en matèria de protecció de dades.

- Coordinar, assessorar i donar suport en la realització de PIA.

6.1.7 Comunicació interna i externa en matèria de privacitat

El DPO tindrà accés als instruments de comunicació existents a l'Entitat amb l'objectiu de fomentar la cultura de compliment. En aquesta tasca compta, així mateix, amb la col·laboració d'aquelles àrees que tinguin responsabilitats en l'àmbit de la comunicació interna. A aquest efecte:

- Les pàgines web de l'Entitat contindran una referència al delegat de protecció de dades.
- El delegat de protecció de dades disposarà d'una secció dins la intranet de l'Entitat a la qual s'inclourà la Política de privacitat, així com qualsevol altra informació que el DPO consideri necessària per al desenvolupament adequat de les seves funcions.

6.1.8 Relacions amb les funcions de control

Als efectes que el delegat de protecció de dades pugui complir les funcions establertes a la normativa, així com a la Política a què fan referència aquests principis, les seves relacions amb altres funcions de control (Compliment Normatiu, Auditoria Interna, Gestió de Riscos) es guiaran pels principis de cooperació i informació recíproca.

Les àrees de control actuaran independentment i sota els seus propis criteris, segons s'estableixi a cada moment a la Política de control intern de l'Entitat, i mantindran coordinació amb el delegat de protecció de dades, facilitant-se mútuament la informació necessària per a la supervisió i el control adequats del compliment del dret de protecció de dades.

Sens perjudici de l'anterior i pel que fa a les facultats de supervisió del compliment de la normativa de protecció de dades:

- El DPO assessorarà la primera línia de defensa pel que fa als controls que cal implementar en les seves àrees respectives en relació amb el compliment de la normativa de protecció de dades, i les àrees o els departaments corresponents seran els encarregats del seu establiment i seguiment.
- La supervisió per part del DPO del compliment de la normativa de protecció de dades es concretarà en la definició i implementació de controls aleatoris i en funció del risc dels tractaments, i tindrà en compte tant la supervisió dels aspectes jurídics com dels aspectes tècnics i de seguretat de la informació.

6.1.9 El delegat de protecció de dades corporatiu

El delegat de protecció de dades de CaixaBank ostentarà la condició de delegat de protecció de dades corporatiu, i tindrà com a responsabilitats, addicionals a les pròpies com a DPO de CaixaBank i de les empreses del perímetre que el nomenin:

- Establir les directrius generals per garantir la gestió adequada del risc de compliment de la normativa de protecció de dades i la implantació de la cultura de compliment en relació amb aquesta normativa al Grup. Així mateix, li correspon establir les directrius generals per tal de garantir una interpretació homogènia de la norma al Grup
- Proposar la creació d'òrgans col·legiats amb abast de Grup
- Promoure el desenvolupament d'un marc de relacions amb els equips de les societats del Grup

- Comunicar tots aquells aspectes que siguin d'interès (lliçons apreses, millors pràctiques, etc.) a les empreses del Grup
- Participar en el nomenament i, si escau, en el cessament dels DPO nacionals de manera que, un cop proposats els candidats o el cessament i els motius, el DPO corporatiu procedirà a remetre el seu informe
- Participar en la fixació de reptes, avaluació de l'exercici i determinació de la remuneració fixa i variable dels DPO nacionals, per a la qual cosa la societat amb presència a l'estranger informarà el DPO corporatiu amb caràcter previ a l'adopció de les decisions corresponents, i aquest últim haurà de remetre el seu informe a la filial
- Participar en i conèixer qualsevol comunicació regular amb els supervisors locals per part de les societats del Grup
- Participar en i conèixer en tot moment l'estat de la gestió de la privacitat a les societats del Grup

6.1.10 Model de govern de la funció de DPO en la presència internacional

CaixaBank, com a capçalera d'un grup que presta serveis financers i d'inversió, té una vocació internacional i s'ha establert en altres jurisdiccions, fora i dins de la Unió Europea, a través de sucursals i oficines de representació. Així mateix, el Grup CaixaBank té presència en altres jurisdiccions a través de filials o en lliure prestació de serveis.

- En el primer cas —la presència de CaixaBank a jurisdiccions fora i dins de la Unió Europea mitjançant l'obertura de sucursals i oficines de representació de CaixaBank—, el delegat de protecció de dades és el de CaixaBank, SA ja que aquestes estructures no tenen personalitat jurídica pròpia.
- En el segon cas —la presència a través de filials o en règim de lliure prestació de serveis—, les societats esmentades del Grup establertes fora d'Espanya hauran de, en cas que ho requereixi la normativa, nomenar un delegat de protecció de dades nacional que compleixi les obligacions següents que l'RGPD estableix:
    - Que el DPO ha de ser expert en la pràctica en matèria de protecció de dades i necessita, en conseqüència, un coneixement expert en cada jurisdicció,
    - Que el DPO ha d'actuar com a punt de contacte i col·laborar amb l'autoritat de control,
    - Que el DPO ha de ser fàcilment accessible pels titulars de les dades des de cada establiment (i, en conseqüència, cal que tingui un coneixement alt de l'idioma local).
- Així mateix, i als efectes d'assolir una aplicació homogènia en cada jurisdicció en què CaixaBank estigui establert, es tractarà de designar al mateix Delegat de Protecció (el Delegat de Protecció de dades nacional) per a totes les filials d'un mateix país.

6.2 Altres figures responsables

6.2.1 Responsable de privacitat

Figura responsable del control i compliment de la normativa de privacitat a cadascuna de les societats del perímetre, nomenat pels òrgans de govern o direcció de cadascuna de les societats. El responsable de privacitat serà el màxim responsable de la gestió de la privacitat a la seva organització. A aquests efectes, es coordinarà amb el delegat de protecció de dades.

Ostentarà la condició de responsable de privacitat qui hagi estat nomenat com a tal pel Comitè de Direcció de la societat. Si no hi hagués nomenament exprés, serà el president del Comitè de Privacitat de la companyia.

6.2.2 Coordinador de privacitat de les àrees o direccions territorials

Figura encarregada d'assessorar en el compliment de la normativa de protecció de dades i realitzar les PIA en les àrees, els departaments, les línies de negoci o les direccions territorials de l'Entitat. Així mateix, és el punt de coordinació i contacte del seu àmbit amb el DPO.

6.3 Tractaments i legitimació

L'Entitat tractarà les dades personals dels interessats per a les finalitats següents:

- "Precontractuals" o "contractuals": per atendre sol·licituds relatives als seus serveis i prestar-los amb la qualitat que s'espera. L'activitat de CaixaBank, com a entitat de crèdit, requereix que s'obtingui determinada informació, s'analitzi, es conservi, s'actualitzi i s'hi accedeixi, en resposta a qui s'interessi per o demani els serveis a l'Entitat. També cal tractar la informació dels candidats i empleats per, si escau, entaular una relació laboral o gestionar-la. El mateix passa en el cas de la relació mercantil que manté amb els seus proveïdors.
- "Reguladores o normatives": per complir les obligacions exigides per les diferents normatives, polítiques i codis, com ara: l'adopció de mesures de diligència deguda en la prevenció del blanqueig de capitals i del finançament del terrorisme, fiscal, de prevenció del frau, sancions internacionals o aquelles obligacions de report requerides per les autoritats reguladores del sector financer.
- "Comercials": l'Entitat pot tractar les dades amb aquesta finalitat basada en l'interès legítim o amb l'autorització prèvia del titular de la dada (consentiment).
- "Organitzatives i de prevenció del frau": l'Entitat pot tractar les dades amb aquesta finalitat segons la necessitat per a l'execució de les relacions contractuals, l'obligació legal o l'interès legítim.

6.4 Drets dels interessats

L'Entitat facilita als interessats l'exercici dels seus drets tal com es defineixen a la normativa de protecció de dades.

Per fer-ho, l'Entitat s'ha dotat dels procediments, així com de les eines i els recursos necessaris, per fer una gestió centralitzada dels drets que li permeti facilitar als interessats l'exercici d'aquests drets mitjançant canals tant físics com digitals. El detall d'aquests procediments es reflectirà actualitzat a la norma de privacitat de l'Entitat.

6.5 Avaluacions d'impacte

Entre els requeriments i les obligacions que estableix l'RGPD destaca la necessitat d'avaluar l'impacte de les activitats de tractament en la protecció de les dades personals sempre que sigui probable que el tractament suposi un risc significatiu per als drets i les llibertats de les persones (PIA).

En aquest sentit, l'Entitat s'ha dotat d'un procediment i d'una metodologia per a la realització de les avaluacions d'impacte esmentades.

Aquest procediment es basa en el principi que tots els tractaments que es facin han de ser detallats pel seu promotor, s'ha de fer una avaluació dels seus riscos i les mesures necessàries per mitigar-los, i la decisió sobre la viabilitat del tractament proposat ha de ser sancionada pel Comitè de Gestió del Risc i Avaluació d'impacte.

El detall d'aquests procediments es reflectirà actualitzat a la norma de privacitat de l'Entitat.

6.6 Mesures tècniques

L'Entitat aplica les mesures tècniques i organitzatives necessàries per mitigar els riscos associats amb la protecció de la informació personal i dels drets i llibertats dels interessats.

Les mesures generals destinades a evitar els riscos relatius a l'alteració, la pèrdua, la no-disponibilitat i el tractament o l'accés no autoritzat a la informació es descriuen a la Política de seguretat de la informació del Grup CaixaBank. Des d'un enfocament preventiu i proactiu es defineixen les mesures que cal aplicar en els sistemes d'informació per protegir la informació en tot el seu cicle de vida. En qualsevol cas, l'aplicació de les mesures concretes serà conseqüència de l'anàlisi i avaluació del risc específic per a cada tractament, seguint la metodologia prevista per a les avaluacions d'impacte (PIA).

A més, l'Entitat i les societats del Grup CaixaBank apliquen un procediment comú per a la gestió de les bretxes o violacions de seguretat de les dades personals, d'acord amb la Política de seguretat de la informació del Grup CaixaBank. Aquest procediment inclou el registre, la gestió i la notificació de les violacions de seguretat de les dades personals a l'AEPD i, quan comportin un risc elevat per als drets i les llibertats, també a l'interessat.

6.7 Proveïdors

L'Entitat s'ha dotat dels procediments, així com de les normes internes necessàries, per fer una selecció responsable dels seus proveïdors d'acord amb el que estableix la normativa de protecció de dades de caràcter personal.

Els procediments de contractació de proveïdors i els contractes de prestació de serveis de l'Entitat incorporen requeriments específics en cas que la prestació de serveis corresponent impliqui el tractament de dades personals, així com mitjans de seguiment i control dels proveïdors.

6.8 Comunicació i formació

Per a l'Entitat és fonamental que els seus empleats, clients i accionistes coneguin el dret a la protecció de dades i siguin conscients de la importància que tenen per a l'Entitat la confidencialitat i el respecte al dret fonamental de la protecció de dades de caràcter personal dels titulars de les dades.

Per això l'Entitat i les societats del grup compten amb un programa de formació intern i extern en virtut del qual es forma els especialistes que assessoren i supervisen en aquesta matèria, liderat pel Delegat de Protecció de dades. Així mateix, el Delegat de protecció de dades lidera el programa formatiu a la resta dels empleats de les Entitats del grup amb caràcter general.

Addicionalment, l'Entitat duu a terme campanyes de conscienciació periòdiques per tal de reforçar el missatge sobre la importància de complir la normativa i les obligacions derivades de la normativa i de la Política a què fan referència aquests principis. En aquest sentit, les campanyes es defineixen en funció dels col·lectius a què es vol conscienciar, com ara clients o empleats, i dins aquesta última categoria també s'adapta al lloc de treball. Així els programes de conscienciació inclouen tant els empleats de la xarxa d'oficines com els coordinadors de privacitat de les àrees, els membres dels diferents comitès i els membres dels òrgans de govern.

En relació amb els proveïdors i el seu personal a què l'entitat pot recórrer per a la prestació de serveis, CaixaBank i les empreses del grup incorporen en les seves relacions contractuals amb aquests la necessitat de formació en matèria de protecció de dades, i a més disposen d'un programa de formació directa per als seus agents i ETT en matèria de protecció de dades.