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

[Març 2022]

Control de versions

Versió	Data	Control
1	[28/03/2022]	Revisió i actualització biennal de la Política Adaptació al model de política corporativa

Contingut

1. Introducció

1.1 Antecedents

Caixabank, SA 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 europeu 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).

Així mateix, mitjançant aquesta Política, el Consell d'Administració 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 a què fan referència aquests principis 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 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 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
- Marc de 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 de *reporting*/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 de la Política a què fan referència aquests principis, 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 filials 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 filials afectades almenys prendran coneixement de l'existència de la Política corporativa a què fan referència aquests principis i de la seva aplicació a les filials esmentades.

En qualsevol cas, la Direcció de Compliance de CaixaBank, atès el seu caràcter corporatiu, vetllarà perquè la integració d'aquesta Política a les filials sigui proporcionada, perquè, en cas que les filials 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.

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.

En el cas de filials o, si escau, sucursals subjectes a jurisdiccions estrangeres o normativa sectorial complementària, les polítiques i els procediments que aquestes filials 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 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 de la privacitat

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 de 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 garantia de seguretat**. La seguretat de la informació és essencial. Per això, es protegirà contra tractaments no autoritzats o il·lícits i contra la pèrdua, la destrucció o el dany accidental.
- **Actuació amb responsabilitat proactiva**. CaixaBank es dotarà dels procediments i les eines necessàries per documentar i conservar totes les accions que dugui a terme, de conformitat amb la Política i la normativa de protecció de dades, pel que fa als tractaments que realitza, per tal no només de complir proactivament la normativa vigent, sinó també per tal d'estar, en tot moment, en disposició d'acreditar el compliment.

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 CaixaBank 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 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.

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.

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,.
- 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 i regulador 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 en aquesta Política, 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 empreses 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).

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 corresponent.

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 imparteix formació periòdicament als seus empleats sobre protecció de dades.

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 d'aquesta Política.