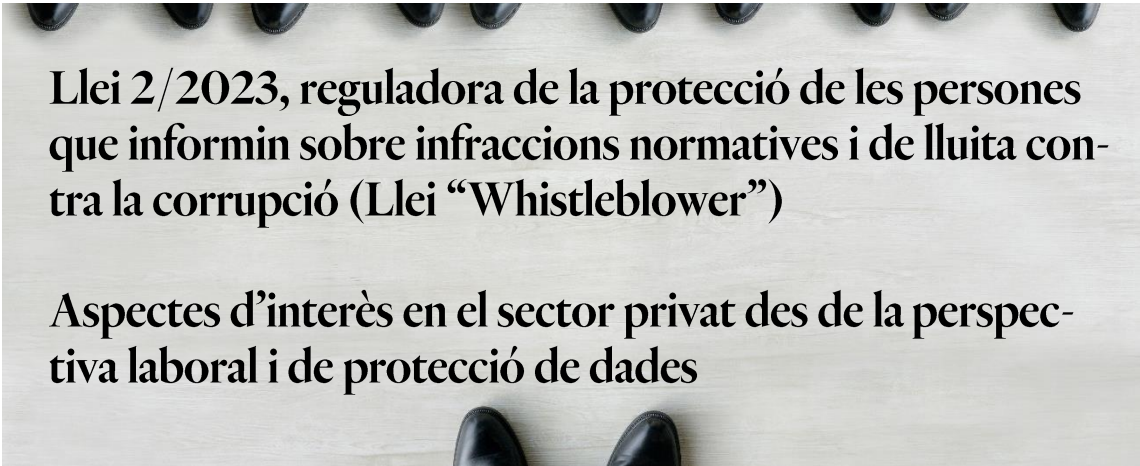


RocaJunyent Informa

Departament Dret Laboral i Protecció de Dades

09 de Març de 2023



Llei 2/2023, reguladora de la protecció de les persones que informin sobre infraccions normatives i de lluita contra la corrupció (Llei “Whistleblower”)

Aspectes d’interès en el sector privat des de la perspectiva laboral i de protecció de dades

El 13 de març de 2023 entra en vigor la **Llei 2/2023, reguladora de la protecció de les persones que informin sobre infraccions normatives i de lluita contra la corrupció** (BOE de 21 de febrer de 2023). Aquesta alerta informativa complementa l’elaborada i publicada pel nostre departament de Laboral el [21 de febrer de 2023](#) i també aborda la perspectiva de protecció de dades.

La citada Llei **transposa la Directiva (UE) 2019/1937**, de 23 d’octubre de 2019, relativa a la protecció de les persones que informin sobre infraccions del Dret de la Unió (d’ara endavant, “Directiva 2019/1937”), coneguda com a “**Directiva Whistleblowing**”.

La **finalitat de la norma** és protegir les persones que, en un context laboral o professional, hagin obtingut informació sobre accions o omissions que puguin constituir **infraccions del Dret de la Unió Europea**¹, així com accions o omissions que puguin ser constitutives **d'infracció penals o administrativa greus² o molt greus i que informin sobre aquestes³**. En tot cas, s'entendran compreses totes aquelles infraccions penals o administratives greus o molt greus que impliquin crebant econòmic per a la Hisenda Pública i per a la Seguretat Social.

La protecció prevista en aquesta llei per a les persones treballadores que informin sobre **infraccions del Dret laboral en matèria de seguretat i salut en el treball**, s'entén sense perjudici del que s'estableix en la seva normativa específica.

És important destacar, des de la perspectiva laboral, que queden expressament **excloues de la protecció prevista en aquesta llei** aquelles persones que comuniquin o revelin informacions vinculades a **reclamacions sobre conflictes interpersonals** o que afectin únicament l'informant i a les persones a les quals es refereixi la comunicació o revelació.

Aquesta llei preveu mecanismes i procediments aplicables a les informacions obtingudes en el marc d'una activitat laboral o professional, així com mesures destinades a protegir els informants (en aquesta Alerta s'utilitza indistintament el terme "denunci-ant").

¹ Sempre que (i) entrin en l'àmbit d'aplicació dels actes de la Unió Europea enumerats en la Directiva 2019/1937 (contractació pública; serveis, productes i mercats financers, prevenció del blanqueig de capitals i el finançament del terrorisme; seguretat dels productes i conformitat; seguretat del transport; protecció del medi ambient; protecció enfront de les radiacions i seguretat nuclear; seguretat dels aliments i els pinsos, sanitat animal i benestar dels animals; salut pública; protecció dels consumidors; protecció de la privacitat i de les dades personals, i seguretat de les xarxes i els sistemes d'informació; (ii) infraccions que afectin els interessos financers de la Unió; infraccions relatives al mercat interior, incloses les infraccions de les normes de la Unió en matèria de competència i ajudes atorgades pels Estats, així com (iii) les infraccions relatives al mercat interior en relació amb els actes que infringeixin les normes de l'impost de societats o a pràctiques la finalitat de les quals sigui obtenir un avantatge fiscal que desvirtuï l'objecte o la finalitat de la legislació aplicable de l'impost de societats.

² S'ha ampliat l'àmbit d'aplicació material de la Directiva 2019/1937 a les infraccions de la legislació nacional, però limitant-ho a les infraccions penals i a les infraccions administratives greus o molt greus, amb la finalitat de permetre als canals d'informació, tant interns com externs, concentrar la seva activitat investigadora en les infraccions de la legislació nacional que es considera que tenen un major impacte en la societat en el seu conjunt.

³ La protecció prevista en aquesta llei no serà aplicable a la informació classificada i tampoc afectarà la protecció del secret professional dels professionals de la medicina i de l'advocacia, al deure de confidencialitat de la Forces i Cossos de Seguretat, així com al secret de les deliberacions judicials.

Les **empreses a partir de 50 empleats**⁴ hauran de crear un **Sistema intern d'informació** ("SII").

La implantació del SII ha de ser impulsat per l'òrgan d'administració i ha de **comptar amb un Responsable del Sistema** (directiu de l'empresa, podent recaure en la persones actualment responsables de la funció de compliment normatiu o polítiques d'integritat). **El SII haurà d'integrar els diferents canals d'informació existents en l'empresa**⁵.

És obligatori permetre les **denúncies anònimes** i la seva tramitació com a tals.

S'estableix així mateix un **canal extern d'informació**⁶ a través de l'**Autoritat Independent de Protecció de l'Informant** (o autoritats o organismes autonòmics corresponents que puguin assenyalar-se en cada CCAA), que podem denominar "canal extern de denúncia", perquè totes les persones físiques puguin informar de la comissió de qualsevol de les accions o omissions incloses en l'àmbit d'aplicació d'aquesta llei.

Es pot acudir directament a aquest canal extern o prèvia comunicació a través del corresponent canal intern. El funcionament d'aquest canal extern es desenvolupa en els articles 17 a 21 de la norma.

És rellevant destacar que aquest "canal extern" nacional és compatible amb la informació per part de les persones físiques davant les institucions, òrgans o organismes pertinenents de la Unió Europea, en cas d'infraccions que entrin en l'àmbit d'aplicació de la Directiva 2019/1937 (això és, per a infraccions del Dret de la Unió Europea).

D'altra banda, es regula la **revelació pública** d'informacions. Es pot fer una divulgació pública en els mitjans de comunicació o en les xarxes socials, etc., amb la protecció establerta en aquesta norma, en els següents suposats:

- (i) quan s'hagin utilitzat els canals interns i/o externs sense que s'hagin pres mesures apropiades sobre aquest tema en el termini establert;

⁴ També estan obligades, amb independència del nombre de persones treballadores, (1) les persones jurídiques del sector privat que entrin en l'àmbit d'aplicació dels actes de la Unió Europea en matèria de serveis, productes i mercats financers, prevenció del blanqueig de capitals o del finançament del terrorisme, seguretat del transport i protecció del medi ambient a les que es refereixen les parts I.B i II de l'annex de la Directiva 2019/1937; (2) els partits polítics, els sindicats, les organitzacions empresarials i les fundacions creades pels uns i els altres, sempre que rebin o gestionin fons públics.

⁵ Els canals interns d'informació podran estar habilitats per l'entitat que els gestioni per a la recepció de qualsevol altres comunicacions o informacions fora de l'àmbit establert en aquesta Llei, si bé aquestes comunicacions i els seus remitents quedaran fora del seu àmbit de protecció.

⁶ La implementació efectiva del canal extern (nacional o autonòmic) està pendent de desenvolupament.

- (ii) quan existeixin motius raonables per a pensar que la infracció pot constituir un perill imminent o manifest per a l'interès públic, existeixi risc de represàlies o hi hagi poques probabilitats que es doni un tractament degut a la informació per les circumstàncies particulars del cas.

Finalment, destaquem que la Llei estableix **un marc sancionador propi** per a l'incompliment de les mesures previstes en aquesta, preveient un conjunt d'infraccions administratives lleus, greus i molt greus, **amb multes de fins a 300.000€ per a persones físiques i de fins a 1.000.000€ per a persones jurídiques**. Així mateix, s'estableixen penalitzacions accessòries en cas d'infracció molt greu, com ara la **impossibilitat de contractar amb l'Administració**.

Davant la imminent entrada en vigor de la norma, continuació, desgranem els aspectes de major interès des de la perspectiva laboral i de protecció de dades, centrant-nos en els Sistemes interns d'informació en el sector privat:

1. Nova obligació empresarial: Sistema intern d'informació (SII)

Les empreses a partir de 50 empleats hauran de crear un Sistema intern d'informació (d'ara endavant, "SII"), o adaptar els ja existents als requeriments d'aquesta norma.

El **termini per a la seva efectiva implementació o adaptació** serà el següent:

- **Empreses amb 250 o més persones treballadores:** fins al 13 de juny de 2023 (tres mesos des de l'entrada en vigor de la Llei).
- **Empreses d'entre 50 i 249 persones treballadors:** fins a l'1 de desembre de 2023.

L'òrgan d'administració serà el responsable de la implantació del SII i tindrà la condició de responsable del tractament de dades personals.

El SII deurà:

- i) Permetre comunicar les infraccions previstes en aquesta norma.
- ii) Garantir la confidencialitat de la identitat de l'informant i de qualsevol tercer esmentat en la comunicació, i de les actuacions que es desenvolupin en la gestió i tramitació de la comunicació.
- iii) Garantir la protecció de dades.
- iv) Impedir l'accés de personal no autoritzat.
- v) Integrar els diferents canals interns d'informació que puguin existir en l'empresa.

- vi) Garantir que les comunicacions presentades es tractin de manera efectiva amb l'objectiu que el primer a conèixer la possible irregularitat sigui la pròpia entitat.
- vii) Ser independent i aparèixer diferenciat respecte dels sistemes interns d'informació d'altres entitats.
- viii) Comptar amb un Responsable del Sistema.
- ix) Comptar amb una política o estratègia que enuncii els seus principis generals i els de defensa de l'informant. Aquesta política o estratègia ha de ser degudament publicitada en el si de l'entitat.
- x) Comptar amb un procediment de gestió de les informacions rebudes.
- xi) Establir garanties per a la protecció dels informants en l'àmbit de l'entitat.

Els sistemes interns de comunicació i els seus corresponents canals que, a l'entrada en vigor d'aquesta llei, tinguin habilitats les empreses podran servir per a donar compliment a les previsions d'aquesta llei sempre que s'ajustin als requisits establerts en la mateixa en els terminis indicats (Disposició transitòria primera i segona de la Llei 2/2023).

No s'exigeix un format específic per al canal, sempre que compleixi els requisits de seguretat, confidencialitat i protecció de dades previstes en la Llei 2/2023.

Els diferents canals interns d'informació que puguin existir en l'empresa (per exemple, contra l'assetjament, de prevenció de delictes, etc.) hauran d'integrar-se en el SII.

2. El SII s'ha de recordar amb la representació legal de les persones treballadores?

No és necessari acordar-ho, però sí que s'exigeix consulta prèvia amb la representació legal de les persones treballadores ("RLPT") abans de la seva implantació per part de l'empresa. Mancant una regulació específica, entenem aplicable l'article 64.6 de l'Estatut dels Treballadors ("ET"), que en línies generals estableix que s'ha de facilitar a la RLPT la informació necessària perquè pugui procedir al seu examen i preparar, si escau, la consulta i informe.

La consulta ha de permetre a la RLPT reunir-se amb l'empresa i obtenir una resposta justificada al seu eventual informe. El termini amb el qual compta la RLPT per a poder emetre el seu informe és d'un màxim de 15 dies.

3. Hi ha alguna previsió específica per als grups de societats?

En el cas d'un grup d'empreses conforme a l'article 42 del Codi de Comerç, l'empresa matriu aprovarà una política general relativa al SII i a la defensa de l'informant, i assegurarà l'aplicació dels seus principis en totes les entitats que l'integren, sense perjudici de la independència i autonomia de cada societat, subgrup o conjunt de societats integrants que, si s'escau, pugui establir el respectiu sistema de govern corporatiu o de governança del grup.

Per tant, **en el cas de grup de societats conforme a l'art. 42 del Codi de Comerç, el SII pot ser un per a tot el grup.**

Hauran no obstant això d'actualitzar-se els acords en matèria de protecció de dades per a la comunicació de dades entre empreses del grup, a fi de recollir aquest nou tractament (i en el seu cas, el règim de corresponsabilitat).

4. Es pot compartir entre diverses empreses el SII?

Las **empresas** que tinguin **entre 50 i 249 persones treballadores poden compartir el SII**, així com els recursos destinats a la gestió i tramitació de les comunicacions (que pot ser gestionat de manera interna per qualsevol d'elles o de forma externalitzada).

Si es determinen conjuntament els mitjans i la forma de gestió, així com els canals que s'integraran, ser necessari subscriure un acord de corresponsabilitat conforme a l'article 26 del Reglament 2016/679, General de Protecció de Dades.

5. Responsable del Sistema intern d'informació (SII)

L'**òrgan d'administració** serà el **competent per a la designació** de la persona física responsable del Sistema i de la **seva destitució** o cessament. Si s'opta per un òrgan col·legiat, aquest ha de delegar en un dels seus membres les facultats de gestió del SII i de tramitació d'expedients de recerca.

El **nomenament** i, en el seu cas **cessament**, del Responsable del SII **haurà de notificar-se a l'Autoritat Independent de Protecció de l'Informant** ⁷ (o autoritats o òrgans competents de les CCAA) en el termini dels 10 dies hàbils següents.

El Responsable del Sistema **haurà de desenvolupar les seves funcions de manera independent i autònoma** respecte de la resta d'òrgans de l'entitat.⁸ Haurà de disposar

⁷ El cessament exigeix especificar les raons que han justificat el mateix.

⁸ No podrà rebre instruccions de cap mena en el seu exercici.

de tots els **mitjans personals i materials** necessaris per a dur a terme les seves funcions.

En el cas de grup de societats conforme a l'art. 42 del Codi de Comerç, el Responsable del Sistema pot ser un per a tot el grup.

6. Qui pot ser el Responsable del SII?

Una persona **directiva de l'entitat**. Quan la naturalesa o la dimensió de les activitats de l'entitat no justifiquin o permetin l'existència d'un directiu/va fet que es dediqui exclusivament a ser Responsable del Sistema, serà possible l'acompliment ordinari de les funcions del lloc amb les de Responsable del Sistema.

Pot ser la **persona responsable de la funció de compliment normatiu o de polítiques d'integritat** que ja existís en l'empresa.

7. Procediment de gestió d'informacions ("denúncies")

L'òrgan d'administració aprovarà el procediment de gestió d'informacions, del compliment diligent de les quals respondrà el Responsable del SII.

El **contingut mínim** d'aquest procediment es desenvolupa en l'article 9 de la norma.

8. Principis generals del procediment de gestió d'informacions

El procediment establirà les previsions necessàries perquè el SII i els canals interns d'informació existent compleixin amb els requisits establerts en la llei. S'estableixen els següents principis i el següent contingut mínim:

- a) Identificació del canal o canals interns d'informació als quals s'associa.
- b) Inclusió d'informació clara i accessible sobre els canals externs d'informació abans les autoritats competents i, en el seu cas, davant les institucions, òrgans o organismes de la Unió Europea
- c) Enviament de justificant de recepció de la comunicació a l'informant dins dels 7 dies naturals següents (tret que això pugui posar en perill la confidencialitat de la comunicació).
- d) Termini màxim per a donar resposta a les actuacions de recerca (3 mesos, amb possibilitat d'extensió fins a un màxim de 3 mesos addicionals en supòsits d'especial complexitat).
- e) Previsió de la possibilitat de mantenir la comunicació amb l'informant i, si es considera necessari, sol·licitar-li informació addicional.

- f) Establiment del dret de la persona afectada al fet que se l'informi de les accions o omissions que se li atribueixen, i a ser sentida en qualsevol moment. Aquesta comunicació tindrà lloc en el temps i forma que es consideri adequat per a garantir la bona fi de la recerca.
- g) Garantia de la confidencialitat quan la comunicació sigui remesa per canals de denúncia que no siguin els establerts o a membres del personal no responsable del seu tractament, al qual s'haurà format en aquesta matèria i advertit de la tipificació com a infracció greu del seu crebant i, així mateix, l'establiment de l'obligació del receptor de la comunicació de remetre-la immediatament al Responsable del Sistema.
- h) Exigència del respecte a la presumpció d'innocència i a l'honor de les persones afectades.
- i) Respecte a les disposicions sobre protecció de dades.
- j) Remissió de la informació al Ministeri Fiscal amb caràcter immediat quan els fets poguessin ser indiciàriament constitutius de delictes. En el cas que els fets afectin els interessos financers de la Unió Europea, es remetrà a la Fiscalia Europea.⁹

9. ¿El canal intern d'informació ha de constar en la pàgina web de l'empresa?

Sí, les empreses han de facilitar informació clara i fàcilment accessible sobre l'ús del canal intern implantat, així com sobre els principis essencials del procediment.

Aquesta informació haurà de constar en la pàgina d'inici de la web de l'empresa, en una secció separada i fàcilment identificable.

Haurà d'incloure's en la informació el **contingut mínim per als interessats respecte del tractament de les seves dades**, conforme al que es disposa en els articles 13 i 14 del Reglament General de Protecció de Dades.

També haurà d'informar-se als empleats sobre el tractament de dades que es realitzarà per raó del SII.

10. Registre d'informacions per part de les empreses

Les empreses hauran de comptar amb un **llibre-registre de les informacions rebudes i de les recerques internes** al fet que hagin donat lloc, garantint en tot cas la confidencialitat.

⁹ Aquesta obligació ha de ser analitzada des de l'òptica del Dret Penal, i pot ser qüestionable per la seva col·lisió, entre altres, amb el dret constitucional a no declarar contra si mateix de l'article 24 de la CE.

Aquest registre no serà públic i només es podrà accedir al seu contingut mitjançant Acte de l'Autoritat judicial competent.

Aquest registre és independent del Registre d'Activitats del Tractament previst en l'art. 30 del Reglament General de Protecció de Dades, i 31 de la Llei orgànica 3/2018 de Protecció de Dades Personals i Garantia dels Drets Digitals (Llei de Protecció de Dades) el qual també **haurà d'actualitzar-se conforme al funcionament i configuració del SII.**

11. Qui pot ser considerat informant, protegit per les garanties de la present norma?

Aquesta llei s'aplicarà als **informants** que treballin en el sector privat o públic i que hagin obtingut informació sobre infraccions en un context laboral o professional, com prenent.

El concepte d'informant és molt ampli, incloent-hi administradors, accionistes, participants, treballadors per compte propi o aliè, ext treballadors, voluntaris, becariis, treballadors en períodes de formació, candidats en processos de selecció o negociació precontractual, autònoms o personal vinculat a empreses contractistes, subcontractistes i proveïdors.

El dret a la protecció atorgada per aquesta llei exigeix que concorrin les circumstàncies següents:

- (i) que les persones que comuniquin o revelin infraccions tinguin motius raonables per a pensar que la informació rebuda és veraç en el moment de la comunicació o revelació, encara que no aportin proves concloents, i que la citada informació entra dins de l'àmbit d'aplicació d'aquesta llei;
- (ii) que la comunicació o revelació s'hagi realitzat conforme als requeriments previstos en la llei.

En canvi, queden expressament **exclosos de la protecció prevista en aquesta llei** aquelles persones que comuniquin o revelin:

- (i) informacions contingudes en **comunicacions que hagin estat inadmeses**;
- (ii) informacions vinculades a **reclamacions sobre conflictes interpersonals** o que afectin únicament l'informant i a les persones a les quals es refereixi la comunicació o revelació, i
- (iii) **informacions que ja estiguin disponibles per al públic o que constitueixin mers rumors.**

12. Els representants legals de les persones treballadores també estan protegits per les garanties de la present norma?

Sí, així com les persones físiques o jurídiques relacionades amb l'informant i que li donin suport, per a prevenir represàlies.

Concretament, **s'estendran les mesures de protecció de l'informant a:**

- a) els **representants legals de les persones treballadores** en l'exercici de les seves funcions d'assessorament i suport a l'informant;
- b) **persones físiques que**, en el marc de l'organització en la qual presti serveis l'informant, **assisteixin al mateix en el procés;**
- c) persones físiques relacionades amb l'informant i que puguin sofrir represàlies, com **companys de treball o familiars de l'informant;**
- d) **persones jurídiques, per a les quals treballi l'informant o amb les quals mantingui qualsevol altre tipus de relació** en un context laboral o en les quals ostenti una participació significativa.

13. Es pot externalitzar la gestió de la recepció de les informacions (“denúncies”)?

Sí. Aquest **tercer extern haurà d'oferir garanties adequades** en matèria d'independència, confidencialitat, protecció de dades i secret de les comunicacions.

Així mateix, **tindrà la consideració d'encarregat del tractament de dades** a l'efecte de la legislació sobre protecció de dades personals i haurà de subscriure l'acord regulat en l'art. 28.3 del Reglament General de Protecció de Dades.

14. Es pot “denunciar” indistintament a través del canal intern o extern?

Sí, les denúncies poden presentar-se **a través de canals interns o externs**, com s'ha exposat.

El canal intern -Sistema intern d'informació (SII)- **és el mitjà preferent per a informar**, sempre que pugui tramitar-se eficaçment i si l'informant considera que no hi ha risc de represàlies.

No obstant l'anterior, **qualsevol persona física podrà denunciar davant "l'Autoritat Independent de Protecció de l'Informant"** (o davant les autoritats o organismes autonòmics competents) bé **directament o prèvia comunicació a través del corresponent canal intern**.

15. Es poden presentar “denúncies” de manera anònima?

Sí, poden presentar-se de manera anònima o amb identificació de l'informant. La tramitació posterior de les comunicacions també pot ser anònima, i en aquest cas ha d'habilitar-se un canal perquè l'informant pugui rebre comunicacions en relació amb la denúncia.

16. Com poden presentar-se les “denúncies” en el canal intern d'informació?

Per escrit, a través de correu postal o a través de qualsevol mitjà electrònic habilitat a aquest efecte, **o verbalment**, per via telefònica o a través d'un sistema de missatgeria de veu. A sol·licitud de l'informant, també podrà presentar-se mitjançant una **reunió presencial** dins del termini màxim de 7 dies¹⁰

Les **comunicacions verbals**, incloses les realitzades a través de reunió presencial, telefònicament o mitjançant sistema de missatgeria de veu, **hauran de documentar-se** d'alguna de les maneres següents, previ consentiment de l'informant:

- a) Mitjançant enregistrament de la conversa en un format segur, durador i accessible, o
- b) A través d'una transcripció completa i exacta de la conversa realitzada per la persona responsable de tractar-la.¹¹

En aquells casos en què la comunicació no sigui remesa pels canals de denúncia establerts o sigui remesa a membres del personal no responsable del seu tractament, el receptor de la comunicació ha de remetre-la immediatament al Responsable del Sistema (art. 9.2.g) de la Llei 2/2023).

¹⁰ En tots aquests formats haurà de proporcionar-se almenys la informació bàsica de primera capa sobre el tractament de dades personals per a complir amb el deure d'informació previst en l'article 13 del Reglament General de Protecció de Dades i l'article 11 de la Llei de Protecció de Dades.

¹¹ S'oferirà a l'informant l'oportunitat de comprovar, rectificar i acceptar mitjançant la seva signatura la transcripció de la conversa.

17. Terminis generals del procés del canal intern d'informació

En un **termini de 7 dies** a partir de la recepció de la comunicació (“denúncia”), ha de **justificar-se recepció a l'informant**, tret que això pugui posar en perill la confidencialitat de la comunicació.

El **termini màxim per a donar resposta a les actuacions de recerca** no podrà ser superior a **3 mesos**, excepte en casos d'especial complexitat, i en aquest cas podrà prorrogar-se altres 3 mesos addicionals.

El termini general de 3 mesos es computa des de la recepció de la comunicació. Si no es va remetre justificant de recepció a l'informant, el termini de 3 mesos es computa des del venciment del termini de 7 dies després d'efectuar-se la comunicació.

S'estableixen terminis específics per a la conservació i supressió de les dades personals i de les comunicacions, en línia amb la normativa de protecció de dades:

- a) han d'eliminar-se tan aviat com deixin de ser necessaris.
- b) Si no es dona curs a la recerca, hauran de suprimir-se tan aviat com es decideixi no donar curs a aquesta, i/o en tot cas, transcorreguts tres mesos des de la recepció de la comunicació sense que s'hagués iniciat la recerca, tret que es preservin amb la finalitat d'evidenciar el funcionament del sistema, i en aquest cas, fins a un màxim de 3 anys¹².
- c) En cap cas poden conservar-se per un termini superior a 10 anys.

18. Accés a les dades personals continguts en el SII

La norma conté un **desenvolupament específic del tractament de dades personals** (articles 29 a 34).

Les dades seran tractades sobre la base del compliment d'obligacions legals, en els casos en què sigui obligatòria la implantació del SII (article 6.1.c del Reglament General de Protecció de Dades), o bé sobre la base del compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable del tractament (article 6.1.e del Reglament General de Protecció de Dades).

Quant a l'**accés a les dades personals continguts en el SII**, quedarà limitat a:

- a) Responsable del SII i qui ho gestioni directament.

¹² Període de prescripció de les infraccions molt greus previstes en aquesta norma.

- b) El responsable de recursos humans o l'òrgan competent degudament designat, només quan pogués procedir l'adopció de mesures disciplinàries contra un treballador.
- c) El responsable dels serveis jurídics de l'entitat, si procedís l'adopció de mesures legals en relació amb els fets relatats en la comunicació.
- d) Els encarregats del tractament que eventualment es designin.
- e) El delegat de protecció de dades.

Serà lícit el tractament de les dades per altres persones, o fins i tot la seva comunicació a tercers, en determinats supòsits taxats: quan resulti necessari per a l'adopció de mesures correctores en l'entitat o la tramitació dels procediments sancionadors o penals que, si escau, procedeixin.

Tot això haurà d'informar-se en la política de privacitat i els procediments interns en matèria de protecció de dades i seguretat de la informació (particularment, els que defineixin els rols i els permisos d'accés als sistemes i les polítiques internes d'empleats).

19. Preservació de la identitat de l'informant

Tota persona que realitzi una comunicació o divulgació pública té **dret al fet que no es reveli la seva identitat a tercers.**

La identitat de l'informant només podrà comunicar-se a l'Autoritat judicial, al Ministeri Fiscal o a l'autoritat administrativa competent en el marc d'una recerca penal, disciplinària o criminal.

20. Prohibició de represàlies contra els informants

Queden expressament prohibits els actes que constitueixin represàlies, incloses les amenaces de represàlies i els intents de represàlies contra els informants.

Es consideraran represàlies, a títol enunciatiu:

- a) Suspensió del contracte de treball, acomiadament o extinció de la relació laboral, inclosa la no renovació o la terminació anticipada d'un contracte de treball temporal després del període de prova; rescissió de contractes de béns o serveis, imposició de qualsevol mesura disciplinària, degradació o denegació d'ascensos i qualsevol altra modificació substancial de les condicions de treball, així com la no conversió d'un contracte de treball temporal en indefinit, tret que aquestes mesures s'hagin dut a terme a l'exercici regular del poder de direcció en virtut de la legislació laboral, per fets o infraccions acreditats i alienes a la presentació de la denúncia.

- b) Danys, inclosos els de caràcter reputacional, o pèrdues econòmiques, coacció, intimidació, assetjament o ostracisme.
- c) Avaluació o referències negatives sobre l'acompliment laboral o professional.
- d) Inclusió en llistes negres o difusió d'informació en un àmbit sectorial concret, que dificultin o impedeixin l'accés a l'ocupació o la contractació d'obres o serveis.
- e) Denegació o anul·lació d'una llicència o permís.
- f) Denegació de formació.
- g) Discriminació, o tracte desfavorable o injust.

El període general de la protecció enfront de represàlies és de dos anys.

21. Presumpció de perjudici en determinats supòsits

En els procediments davant un òrgan jurisdiccional o una altra autoritat en relació amb els danys soferts pels informants, una vegada que l'informant hagi demostrat raonablement que ha comunicat o ha fet una revelació pública de conformitat amb aquesta Llei i que ha patit un perjudici, **es presumirà que el perjudici va ser una represàlia** per informar o fer una revelació pública. En aquests casos, correspon a la persona que ha pres la mitjana perjudicial provar que aquesta mesura es va basar en motius degudament justificats no vinculats a la comunicació o revelació pública.

22. Mesures de protecció de les persones afectades

Durant la tramitació de l'expedient les persones afectades per la comunicació ("persona denunciada") tindran dret a la **presumpció d'innocència, dret de defensa i dret d'accés a l'expedient**, així com a la **mateixa protecció establerta per als informants, preservant-se la seva identitat** i garantint-se la **confidencialitat** dels fets i dades del procediment.

23. Sistema de sancions

Aquesta Llei estableix un **marc sancionador propi** per a l'incompliment de les mesures previstes en la mateixa. L'exercici de la potestat sancionadora correspon a la "Autoritat Independent de Protecció de l'Informant" (o als òrgans competents de les CCAA).

La norma preveu un conjunt d'infraccions administratives lleus, greus i molt greus, amb **multes de fins a 300.000 € per a persones físiques i de fins a 1.000.000 € per a**

persones jurídiques. Es tipifica com a infracció molt greu, entre d'altres, l'incompliment de l'obligació de disposar d'un Sistema intern d'informació en els termes establerts a la Llei (amb multa mínima de 30.001 € per a persones físiques i de 600.001 € per a persones jurídiques).

Adicionalment, en el cas d'infraccions molt greus, es podran acordar **sancions complementàries**: (i) l'amonestació pública; (ii) la prohibició d'obtenir subvencions o altres beneficis fiscals durant un màxim de 4 anys, així com (iii) la prohibició de contractar amb el sector públic durant un màxim 3 anys.

Les sancions per infraccions molt greus imposades a persones jurídiques, una vegada fermes en via administrativa, podran ser publicades en el BOE.