



AVALUACIÓ D'IMPACTE DEL TRACTAMENT DE DADES PERSONALS DEL SERVEI DE GESTIÓ DE RESIDUS

ÍNDEX

1.	INTRODUCCIÓ	3
2.	DESCRIPCIÓ SISTEMÀTICA DE LES OPERACIONS DE TRACTAMENT	4
2.1	NOM I DESCRIPCIÓ DEL TRACTAMENT	4
2.2	IDENTIFICACIÓ DELS RESPONSABLES DEL TRACTAMENT DE LES DADES	4
2.3	DADES PERSONALS TRACTADES	5
2.4	GESTIÓ I PROCESSAMENT DE LES DADES	7
2.5	TRACTAMENT DE LES DADES PER TERCERS	7
2.6	TRANSFERÈNCIES INTERNACIONALS.....	9
3.	ANÀLISIS DE LA NECESSITAT DE REALITZAR AVALUACIÓ D'IMPACTE.....	10
4.	AVALUACIÓ DE LA NECESSITAT I LA PROPORCIONALITAT DE LES OPERACIONS DE TRACTAMENT RESPECTE AMB LA SEVA FINALITAT.....	12
4.1	PRINCIPI D'IDONEÏTAT (ART.5.1 A).....	12
4.2	PRINCIPI DE LICITUD I LLEIALTAT DEL TRACTAMENT.....	12
4.3	PRINCIPI DE MINIMITZACIÓ	18
4.4	PRINCIPI D'EXACTITUD DE LES DADES	19
4.6	PRINCIPI DE LIMITACIÓ DEL TERMINI DE CONSERVACIÓ	20
4.7	NECESSITAT I PROPORCIONALITAT DEL TRACTAMENT	21
4.8	OPINIÓ DELS INTERESSATS	21
5.	AVALUACIÓ DELS RISCOS PER ALS DRETS DELS INTERESSATS.....	22
5.1	IMPACTE.....	22
5.2	PROBABILITAT INICIAL	24
5.3	RISC INICIAL EN EL TRACTAMENT DE DADES.....	25
5.4	MESURES DE SEURETAT	26
6.	CONCLUSIONS	29

1. Introducció

El present document respon a la necessitat de l'Ajuntament de Lliçà d'Amunt (en endavant, l'Ajuntament) de complir amb els requisits expressats en la legislació de protecció de dades i garantir els drets i llibertats de les persones.

En compliment per l'establert pel Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 de abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament i la lliure circulació de dades personals (d'ara endavant, RGPD o Reglament), i d'acord el determinat pels procediments de l'Ajuntament de Lliçà d'Amunt es realitza l'avaluació d'impacte relativa a la protecció de dades (AIPD) del tractament de Gestió de residus i neteja viària.

El present informe compta amb els següents apartats:

1. Descripció sistemàtica de les operacions de tractament
2. Anàlisi de la necessitat de realitzar una AIPD
3. Avaluació de la necessitat i proporcionalitat de les operacions de tractament respecte amb la seva finalitat.
4. Avaluació dels riscos per als drets i llibertats dels interessats.
5. Determinació de les mesures per tal de reduir riscos.
6. Pla d'acció i conclusions

2. Descripció Sistemàtica de les operacions de tractament

Es detalla la descripció del tractament de dades per a la posterior avaluació del compliment dels diferents principis fonamentals del RGPD i valorar el riscs que pugui comportar aquest tractament.

2.1 Nom i descripció del tractament

En aquest apartat s'haurà d'indicar el nom intern, la seva denominació en el Registre d'Activitats de Tractaments i una descripció del tractament incloent la informació establerta en l'article 31 de la LOPDGDD i l'article 30 del RGPD.

Àrea	Tractament	Finalitat del tractament
Regidoria de residus	Gestió de recollida de residus	Prestació dels següents serveis: - Serveis de transport i recollida de residus al terme municipal. - Gestió de la relació de persones usuàries del servei per a l'accés als contenidors.

2.2 Identificació dels responsables del tractament de les dades

La identificació dels responsables i corresponsables del tractament, responsables funcionals i encarregats del tractament és important per tal d'avaluar els riscos i el compliment amb la normativa.

Identificació de la Entitat Responsable	Ajuntament de Lliçà d'Amunt
Identificació de les Entitats Corresponsables (si s'escau)	No aplica
Identificació del punt de contacte/interlocutor de l'Entitat Responsable	Tècnic de medi ambient i salut
Identificació del punt de contacte/responsable funcional de l'Entitat Corresponsable	No aplica

2.3 Dades personals tractades

Les característiques de les dades personals a tractar són rellevants a l'hora de determinar els riscos del tractament i el compliment d'algunes disposicions del reglament i la llei orgànica.

En la següent taula, s'analitzarà de manera conjunta el tipus de dades personals que es tracten des de l'Ajuntament.

Categoria de dades personals	Aplica?
Dades especialment protegides: persones en situació de vulnerabilitat,	NO
Dades identificatives: Nom, cognom, telèfon, adreça postal o electrònica, , signatura (electrònica o manuscrita), DNI/NIF, referència cadastral	SI
Dades tributàries o econòmico-financeres: Ingressos, rendes, dades bancàries, deduccions impositives/impostos/tributs, deduccions per rendes baixes,	NO
Dades acadèmiques i professionals (treball/comercial)	NO
Dades relatives a les circumstàncies socials: Característiques d'allotjament, habitatge, situació familiar (número de membres familiars a l'habitatge), propietats/possessiones, hàbits, (necessitats pel que fa als usos del servei de residus)	NO
Dades relatives a les característiques personals	NO
Dades recollides en l'exercici de la potestat sancionadora	NO

Observacions

Es tractaran les següents dades: nom i cognom, adreça postal, adreça electrònica, telèfon, DNI o NIE, número de document d'identificació personal identificador de l'usuari del servei (targeta o aplicació), referència cadastral.

Col·lectius sobre els quals es recolliran les dades	Aplica?	Observacions
Usuaris del servei	SI	
Personal	NO	
Interlocutors de Persones jurídiques (empreses o AAPP) o entitats sense personalitat jurídica (Associació de veïns i comunitats de propietaris)	SI	
Professionals (autònom)	SI	
Contribuents	SI	
Altres. Especificar el col·lectiu:	NO APLICA	

Observacions

No aplica.

2.4 Gestió i processament de les dades

La manera de tractament de les dades personals són rellevants a l'hora de determinar els riscos del tractament i el compliment d'algunes disposicions del RGPD i la LOPD-GDD.

Origen/Mitjans de recollida de dades	○ Formulari d'inscripció al servei de recollida de residus ○ Cadastre ○ Padró Municipal d'Habitants
Destinatari de les dades	○ Empreses encarregades del tractament ○ Entitats financeres ○ Jutges i tribunals ○
Sistema de tractament de les dades	○ App mòbil ○ Portal web ○ Targeta d'usuari ○ Expedient administratiu i sistemes corporatius de l'Ajuntament
Mesures de seguretat previstes	Les definides a l'ENS i les definides en el plec tècnic que reguli la licitació del servei extern.
Termini de conservació	Definit al Quadre de Classificació Documental de l'Ajuntament.
Ús amb propòsit diferent al de la recollida	No

2.5 Tractament de les dades per tercers

La identificació dels encarregats de tractament de les dades i l'ús que fa de les dades és important a l'hora de determinar els riscos del tractament i el compliment d'algunes disposicions del reglament i la llei orgànica.

Encarregat	Tractament	Tipus de dades	Sistema	Instrument jurídic vinculant
Empresa adjudicatària del LOT 1	Sistema de tancament i accés als contenidors de residus	Nom i cognoms, correu electrònic, telèfon (per a usuaris del sistema mitjançant aplicació al telèfon mòbil), número identificador de la persona usuària del servei.	Aplicatiu i portal web que desenvolupi l'empresa en el marc del contracte de prestació de servei	Contracte de prestació del servei

Empresa adjudicatària del LOT 2	Servei de realització d'una campanya de comunicació sobre el servei	Nom i cognom, adreça postal, adreça electrònica, telèfon.	Aplicatiu i portal web que desenvolupi l'empresa en el marc del contracte de prestació de servei	Contracte de prestació del servei

2.6 Transferències Internacionals

Compartir dades amb agents externs pot incrementar els riscos del tractament; especialment si es fan a tercers països on l'RGPD no aplica.

Es fan transferències de dades a un tercer país, fora de l'Espai Econòmic Europeu?	No
Està previst que l'Encarregat del tractament faci transferències internacionals?	No
La destinació d'aquestes dades es fan a un país que compleix amb les garanties adequades de protecció de dades (instrument vinculant entre autoritats o organismes públics, normes corporatives vinculants, autorització de les autoritats competents (AEPD, APDCAT), codis de conducta, certificacions)?	No aplica
A quina entitat es fa la destinació de les dades?	No aplica
Quines dades es comparteixen?	No aplica
Amb quin motiu es transfereixen les dades?	No aplica
Quin instrument jurídic es vincula aquesta relació?	No aplica
Quines són les garanties establertes per la seguretat de les dades?	No aplica

3. Anàlisi de la necessitat de realitzar avaluació d'impacte

Per a poder determinar si és necessari realitzar una Avaluació d'Impacte s'ha d'analitzar la probabilitat que, per la naturalesa, abast i context el tractament de dades personals pugui tenir un alt risc per als drets i llibertats de les persones físiques, segons els següent barems definits a partir dels principis establerts pel RGPD i el Grup de Treball de l'article 29:

No es donen cap dels supòsits següents:

Supòsit	Aplica?
El tractament té naturalesa, abast, context i finalitat semblant a un altre tractament pel qual ja s'ha fet una AIPD.	No
El tractament té una base jurídica en el dret de la UE o d'un estat membre, i ja s'ha realitzat una AIPD en el moment d'adoptar aquesta base jurídica.	No
Justificació El tractament objecte de la present AIPD encara no està implementat i per tant no ha estat objecte de cap AIPD prèvia per part de l'Ajuntament de Lliçà d'Amunt.	

El tractament no es troba en els supòsits i criteris anteriors que proposa l'Agència Espanyola de Protecció de Dades que ho requereix explícitament.

Per aquest motiu, s'haurà d'analitzar si el tractament en qüestió entra dins dels supòsits de la llista no exhaustiva de tractaments en què sí que és necessari realitzar una AIPD (criteris establerts pel Grup de Treball de l'Article 29 en la guia WP248 *"Directrius sobre l'avaluació d'impacte relativa a la protecció de dades i per a determinar si el tractament comporta un probablement risc alt a efectes del RGPD"*).

Indicador de potencial risc alt dels tractaments	Aplica?
Avaluació o puntuació, incloses l'elaboració de perfils i prediccions sobre aspectes de la seva personalitat o dels seus hàbits	No
Presa de decisions automatitzada amb efectes jurídics o que afecti de manera similar i significativa a la persona física.	No
Observació, monitorització, supervisió, geolocalització o control de l'interessat de manera sistemàtica y exhaustiva (serveis web, aplicacions mòbil, etc.)	Si
Ús de categories especials de dades, dades relatives a condemnes o infraccions penals o dades que permetin determinar la situació financera o de solvència patrimonial o deduir informació sobre categoria especials de dades personals	No
Ús de dades biomètriques amb el propòsit d'identificar de manera única a una persona física	No
Utilització de dades genètiques per a qualsevol fi.	No
Tractament de dades a gran escala	Sí

Associació, combinació o enllaç de registres de bases de dades de dos o més tractaments amb finalitats diferents o per responsables diferents.	Si
Dades relacionades amb persones vulnerables o amb risc d'exclusió social (persones menors, amb discapacitat, que accedeixen a serveis socials i víctimes de violència de gènere)	No
Ús innovador de tecnologies.	No
Tractament que en sí mateix impedeix l'exercici d'un dret o l'ús d'un servei o executar un contracte	No

És necessari realitzar un AIPD? Per quina raó?

Sí, és necessari perquè el tractament apliquen els diferents supòsits que requereixen la anàlisi d'impacte:

- Es tracten **dades a gran escala**, ja que es tracten les diverses dades de tots els ciutadans de Lliçà d'Amunt per tal de portar a terme la prestació del servei de recollida de residus i servei de deixalleria.
- **S'associen registres de bases de dades de dos o més tractaments amb finalitats diferents** perquè s'utilitza la base de dades que deriva de la recollida de dades mitjançant el formulari de d'inscripció al servei de recollida de residus amb les dades del Cadastre i del Padró Municipal d'Habitants. Aquesta associació de dades de diferents tractaments està justificada per la normativa vigent (la Llei Reguladora de las Bases del Règim Local).
- Aquest servei podria comportar **presa de decisions automatitzada amb efectes jurídics o que afecti de manera similar i significativa a la persona física**, atès que depenent dels usos i/o pràctiques de la gestió dels residus de cada persona la taxa a pagar pot variar.

Per tots aquests motius és necessari portar a terme un AIPD del tractament del servei de recollida de residus i deixalleria.

4. Avaluació de la necessitat i la proporcionalitat de les operacions de tractament respecte amb la seva finalitat

L'avaluació de la necessitat i de la proporcionalitat del tractament es fa en relació a la finalitat del tractament, que s'ha descrit a la secció anterior.

L'objectiu d'aquest apartat és avaluar si el tractament compleix amb els diferents principis que preveu l'article 5 del RGPD: principi d'idoneïtat de manera que les dades es recullin amb fins determinats, explícits i legítims; principi de licitud, lleialtat; principi de minimització de les dades; principi d'exactitud de les dades; principi de limitació de conservació de les dades; tractats de tal manera que es garanteixi una seguretat adequada de les dades personals.

4.1 Principi d'idoneïtat (art.5.1 a)

D'acord amb la legislació vigent, les dades recollides s'han d'utilitzar per a assolir la finalitat del tractament que va motivar la recollida, és a dir, les dades s'han de recollir amb fins determinats, explícits i legítims, i no hauran de ser tractats ulteriorment de manera incompatible amb aquests fins. Ara bé, en alguns casos, el Reglament permet el tractament de dades que han estat recollides amb una finalitat diferent.

Es preveu utilitzar dades recollides amb una finalitat diferent a la del tractament previst?	NO
--	----

4.2 Principi de licitud i lleialtat del tractament

Les dades s'han de tractar de manera lícita, lleial i transparent en relació amb l'interessat.

Base legitimadora

Un tractament és lícit si aplica alguna de les bases legals següents:

L'interessat ha donat el seu consentiment per al tractament de les seves dades personals, per una o diverses finalitats específiques.	SI
El tractament és necessari per executar un contracte en què l'interessat n'és part o per aplicar mesures precontractuals.	NO
El tractament és necessari per complir una obligació legal aplicable al responsable del tractament.	NO
El tractament és necessari per protegir interessos vitals de l'interessat o d'una altra persona física.	NO
El tractament és necessari per complir una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable del tractament.	SI
El tractament és necessari per satisfer els interessos legítims del responsable del tractament o d'un tercer, sempre que no hi prevalguin els interessos o els drets i les llibertats fonamentals de l'interessat (en particular, quan l'interessat és un menor).	NO
Justificació de la licitud del tractament	

El tractament del servei de recollida selectiva està justificat l'exercici de les competències municipals previstes en l'article 84.2 apartat a) i c) de l'Estatut d'Autonomia de Catalunya, l'article 25.2 apartats b) i b) de la Llei reguladora de les Bases de Règim Local i l'article 66.3 apartats d) i l) de la Llei Municipal i de règim local de Catalunya en matèria de residus.

Així mateix, les persones usuàries del servei mitjançant l'atorgament del seu consentiment via formulari comunicaran quins usos sol·liciten en relació a la recollida de residus de l'Ajuntament.

S'ha portat a terme un anàlisi de no incórrer en cap tractament il·lícit en un sentit més ampli:

Possibles legislacions i drets afectats	Licitud
Drets d'autor (drets patrimonials o morals d'una creació d' una obra literària, artística, musical, científica, arquitectònica o didàctica)	SI
Drets de propietat industrial (marques, patents, dissenys industrials i dibuixos)	SI
Convenis i acords contractuals	SI
Drets de la competència o protecció dels secrets empresarials	SI
Altres	SI

Observacions

La app mòbil i portal web seran creades a mida per part de l'encarregat del tractament , sense necessitat d'adquirir cap llicència d'ús.

La resta de legislacions i drets que puguin estar afectats no apliquen.

Tractament de dades de menors

Els menors necessiten una protecció especial en el tractament de les seves dades, perquè poden no ser conscients dels riscos que comporta.

El tractament ofereix serveis de la societat de la informació a nens i té com a base el consentiment?	No
En cas afirmatiu, s'ha tingut en compte l'edat mínima de consentiment?	No aplica
S'ha tingut en compte si d'acord amb el tipus de tractament de dades el menor o els seus pares/mares/tutors legals han de atorgar el seu consentiment?	No aplica

Observacions No aplica.
--

Tractament de categories especials de dades

En virtut de l'article 9 del RGPD, queden prohibits els tractaments de dades personals que revelin l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques, la afiliació sindical, les dades genètiques, les dades biomètriques dirigides a identificar de manera unívoca a una persona física, dades relatives a la salut, dades relatives a la vida sexual o orientació sexual d'una persona física.

Es tracten dades de categories especials?	No
---	----

En cas afirmatiu	
El tractament de categories especials de dades està prohibit, llevat que apliqui algun dels supòsits següents.	
L'interessat ha donat el seu consentiment explícit per al tractament amb una finalitat específica, tret que el dret de la UE o de l'estat membre no ho permeti.	
El tractament estigui emparat per una norma amb rang de llei	
El tractament és necessari per complir obligacions o per exercir drets en l'àmbit del dret laboral i de la seguretat i la protecció social.	
El tractament és necessari per protegir interessos vitals de l'interessat o d'una altra persona, i l'interessat no està capacitat per donar el consentiment.	
El tractament és legítim i amb garanties, fet per una associació sense ànim de lucre de caràcter polític, filosòfic, religiós o sindical, sempre que el tractament afecti persones amb qui mantenen contactes en relació amb aquestes finalitats i les dades no es comuniquin a tercers sense el consentiment dels interessats.	
El tractament fa referència a dades que l'interessat ha fet públiques.	
El tractament és necessari per formular, exercir o defensar reclamacions, o quan els tribunals actuen en la seva funció judicial.	
El tractament és necessari per raons d'interès públic essencial.	
El tractament és necessari per a finalitats de medicina preventiva o laboral, avaluació de la capacitat laboral del treballador, diagnòstic mèdic, prestació d'assistència o tractament de tipus sanitari o social, en cas que així ho exigeixi la gestió dels sistemes i serveis d'assistència sanitària i social, pública i privada, o l'execució d'un contracte d'assegurança de que l'afectat sigui part.	

El tractament és necessari per raons d'interès públic en l'àmbit de la salut pública.	
El tractament és necessari amb la finalitat d'arxiu amb interès públic, investigació científica o històrica, o amb finalitat estadística.	
Justificació de la licitud del tractament de dades de categories especials.	
No aplica.	

Observacions No aplica.
--

Tractament de dades personals relatiu a condemnes i infraccions penals

Es tracten dades relatives a condemnes o infraccions penals?	No
--	-----------

Lleialtat del tractament

Un tractament és lleial si fa un ús de les dades previsible per part dels interessats, i del tractament no se'n deriven conseqüències adverses pels interessats que no siguin justificables.

Justificació de tractament lleial

El tractament de dades amb la finalitat de gestió de residus es porta a terme de manera lleial perquè existeix una base jurídica que ho habilita, l'exercici de les competències municipals i el consentiment de la persona interessada.

Aquest ús és previsible per part dels usuaris del servei, ja que per la prestació d'un servei és necessari que es tractin les dades personals.

4.3 Principi de minimització

Les dades han de ser adequades, rellevants i limitades a l'estrictament necessari per aconseguir la finalitat del tractament.

Tipus de dades	
	nom i cognom, adreça postal, adreça electrònica, telèfon, DNI o NIE, número de document d'identificació personal identificador de l'usuari del servei (targeta o aplicació), referència cadastral.

Justificació de l'adequació, la rellevància i la necessitat

Es recull la informació mínima i necessària per a portar a terme el servei de recollida selectiva i deixalleria, d'acord l'anàlisi realitzat per l'autor d'aquest informe.

Sense aquesta informació no es podria portar a terme el servei.

La informació és la imprescindible per a portar a terme:

- Alta a l'aplicació APP mòbil (nom i cognom, adreça electrònica i telèfon).
- Alta presencial per a l'assignació de la targeta associada a la persona usuària, on l'empresa gestora del servei tindrà accés al conjunt de dades identificades a l'apartat *Tipus de dades*.

4.4 Principi d'exactitud de les dades

El principi d'exactitud estableix que les dades han de ser exactes i que el responsable de les dades ha de prendre mesures raonables per garantir que les dades siguin exactes i s'actualitzin, rectifiquin o s'esborrin sense dilació.

Tipus de controls de la qualitat de les dades

Les dades s'actualitzen regularment d'acord la informació del Padró, del Cadastre, la supervisió presencial de l'Ajuntament, l'alta a l'aplicació APP mòbil i el portal web; garantint la veracitat de les dades.

La informació actualitzada es recollirà a l'aplicació APP mòbil i el portal web, garantint al contracte d'encarregat de tractament que l'allotjament de les dades serà dins de la Unió Europea.

Mesures correctives de l'exactitud les dades

La regidoria de Residus, directament o per mitjà dels tercers contractats, haurà de portar a terme les accions d'actualització de la informació que garanteixi l'exactitud de les dades; ja sigui per mitjans automatitzats o manuals.

4.6 Principi de limitació del termini de conservació

Les dades personals no s'han de conservar més temps de l'estrictament necessari per complir amb la finalitat del tractament.

Justificació que els terminis de conservació donats compleixen amb la limitació del termini de conservació.

El temps de conservació de les dades de cada document està vinculat a les normes de conservació de dades/prescripció de les sancions previstes en la legislació vigent i recollida de manera exhaustiva en el Quadre de Classificació de l'Ajuntament de Lliçà d'Amunt.

- Llei 58/2003, de 17 de desembre, General Tributària
- Llei 39/2015, d'1 d'octubre, de procediment administratiu comú de las administracions públiques.
- Llei 29/1998, de 13 de juliol, reguladora de la jurisdicció contenciosa-administrativa.
- Reial decret legislatiu 2/2004, de 5 de març, pel qual s'aprova el text refós de la Llei reguladora de les hisendes locals

Descripció dels mecanismes establerts per esborrar les dades

Un cop transcorregut el període establert al Quadre de Classificació de l'Ajuntament de Lliçà d'Amunt, les dades seran esborrades i per tant, no podran ser utilitzades.

Es conserven dades amb finalitat d'arxiu en interès públic, amb finalitat d'investigació científica o històrica, o amb finalitat estadística.

Sí

Es podrien tractar les dades amb finalitat estadística, com així ho preveu l'article 5, apartat 1, lletra b), article 6, apartat 4, i article 89, apartat 1 i considerants 39 i 50 del Reglament General Europeu de Protecció de Dades Personals.

La finalitat estadística del tractament de gestió de servei de recollida selectiva i deixalleria és compatible, ja que es podria portar a terme únicament per poder millorar el servei que s'ofereix als usuaris del servei.

4.7 Necessitat i Proporcionalitat del Tractament

Justificació de la necessitat del tractament.

La recollida de dades personals és necessària per poder portar a terme el servei de i donar compliment a la legislació que obliga a disposar d'informació sobre la generació de residus de cada unitat, ja que sense aquestes no seria possible.

No existeix cap altra mesura per portar a terme el servei que no sigui tractar dades personals.

Les dades que es recullen són les mínimes i imprescindibles.

Justificació de que el tractament és proporcional

Es delimita el tractament de dades personals als tràmits necessaris per poder portar a terme el servei i només les dades mínimes necessàries.

4.8 Opinió dels interessats

L'RGPD estableix que, si és possible, cal recollir l'opinió dels interessats sobre el tractament.

Opinió dels interessats sobre la necessitat i la proporcionalitat del tractament.

No s'ha recollit

En cas que no es considera apropiat recollir l'opinió dels interessats, cal justificar-ho.

Per què no s'ha recollit l'opinió dels interessats?

Com és un tràmit definit per una competència municipal, es considera suficientment justificat de forma legal el seu tractament; respectant els principis d'idoneïtat; principi de licitud, lleialtat; principi de minimització de les dades; principi d'exactitud de les dades; principi de limitació de conservació de les dades.

El tractament es porta a terme de tal manera que es garanteixi una seguretat adequada de les dades personals.

5. Avaluació dels riscos per als drets dels interessats

A continuació s'avalua i identifiquen els possibles efectes negatius sobre les persones derivats del tractament de dades motiu de l'avaluació.

L'anàlisi de riscos s'ha portat a terme considerant el tractament i el cicle de vida de les dades.

El risc s'ha determinat considerant dos factors:

- Impacte sobre la intimitat i la privacitat de les persones
- Probabilitat que succeeixi

El risc es determina com a resultat directe de l'impacte i de la probabilitat

5.1 Impacte

L'impacte del tractament s'avalua analitzant en la pèrdua de la confidencialitat, de la integritat i de la disponibilitat de les dades personals sobre els interessats en determinats escenaris.

Amb el següent criteri:

IMPACTE	DESCRIPCIÓ
Acceptable (baix)	Poc o cap efecte
Tolerable	Els efectes se senten però no són crítics
No desitjable	Impacte seriós en el curs d'acció i el resultat
Intolerable	Podria resultar un desastre

Per a cadascuna de les dimensions de seguretat:

Confidencialitat: accés no autoritzat o difusió pública
Els escenaris contemplats atès el tractament i sistema empleat són: • Pèrdua o robatori de documentació amb la informació dels usuaris. • Vulneració del canal de comunicació. • Enviament per error de dades personals a sistemes diferents del definit. • Possibilitat d'accedir de forma no autoritzada al servidors municipals o dels prestadors de serveis. • Difusió no autoritzada de la informació en els sistemes d'informació. • Robatori d'informació (lògica o física) dels servidors de l'encarregat del tractament. • Accés per perfils no autoritzats per error de configuració o permisos.
Impacte: Alt (No desitjable)
Justificació: La divulgació de dades personals podria suposar la difusió potencial de les dades de tota la població usuària del servei municipal.

Aquesta potencial afectació a la confidencialitat suposaria un accés a dades massives responsabilitat de l'Ajuntament.

Integritat: modificació no autoritzat de les dades

Els escenaris contemplats atès el tractament i sistema empleat són:

- Modificació errònia accidental o intencionada de les dades per part de personal autoritzat.
- Error en les comunicacions impliquen alteració de les dades entre la informació recollida pels prestadors de serveis o l'ajuntament i la conservada als sistemes.
- Modificació per un atac cibernètic.

Impacte: Mitjà (Tolerable)

Justificació: La modificació de les dades podria suposar una afectació sobre els drets de les persones, podent implicar una reducció significativa de les obligacions dels serveis (inclouen la impossibilitat de lliurar el servei) i podent suposar un perjudici als usuaris.

Això no obstant, en tant que la pèrdua d'integritat es detectaria en el moment d'una incorrecta facturació o prestació del servei, la disponibilitat de còpies de seguretat i dels documents (contractes, etc.) originals permetrien solucionar aquests problemes.

Disponibilitat: impossibilitat d'accés a les dades

Els escenaris contemplats atès el tractament i sistema empleat són:

- El servei deixa d'estar disponible (caiguda del hosting per diverses causes: problema de comunicacions, programari, maquinari, alimentació elèctrica, etc.)
- La informació es va malbé i no hi ha possibilitat de recuperació.

Impacte: Mitjà (Tolerable)

Justificació: La manca d'accés a les dades suposaria la impossibilitat de prestar els serveis als usuaris el període d'incapacitat d'accedir a aquestes. Això no obstant – des del punt de vista de tractament de dades – l'accés a les dades pels usuaris no és un requeriment imprescindible per a rebre el servei de recollida selectiva; tot i que sí imprescindible per a la gestió del servei i cobrament de taxes.

En aquest sentit la indisponibilitat no suposaria la incapacitat de prestar el servei – que disposa de mecanismes redundants i pla de contingència - si no la de la gestió administrativa del servei.

Qualsevol indisponibilitat d'accés a les dades podria ser realitzat amb posterioritat de la recuperació, es tracti de facturació, ajuts o altres actuacions.

L'impacte resultant és el major dels tres: No desitjable

Aquesta valoració ve donada per la possible difusió o accés per tercers de dades personals en cas de vulneració de la Confidencialitat d'un ampli col·lectiu de persones (tot el conjunt de persones usuàries del servei es consideraria un tractament de dades massiu).

5.2 Probabilitat Inicial

La probabilitat es determina de l'exposició, tecnologia empleada i l'organització:

Paràmetre	Valor
Tecnologia	
El sistema de tractament està connectat a sistemes externs a l'organització?	SI
Alguna part del tractament es fa a través d'internet?	SI
Manca de seguiment d'un document de bones pràctiques rellevant en el disseny o la configuració del sistema de tractament?	NO
Manca de seguiment d'un document de bones pràctiques rellevant en el manteniment, la monitorització i la resposta a incidents del sistema de tractament?	NO
Hi ha una manca de seguretat física a les instal·lacions on té lloc el tractament?	NO
Ús del sistema de tractament	
Hi ha una manca de claredat en la definició dels rols i les responsabilitats dels treballadors?	NO
Hi ha manca de claredat en la definició dels usos acceptables dels sistemes de tractament?	NO
Pot el personal connectar dispositius externs al sistema?	NO
Manca un procediment adequat de registre i supervisió de les activitats relacionades amb el tractament?	NO
Persones que intervenen en el tractament	
El personal rep permisos que no són necessaris per complir les tasques que té encomanades?	NO
S'ha externalitzat alguna part del tractament a un encarregat?	SI
Hi ha una manca de coneixement del personal respecte de l'ús adequat del sistema, d'aspectes de seguretat de les dades o de les limitacions d'ús que imposa l'RGPD?	NO
Altres característiques	
Ha patit l'entitat o altres del sector atacs darrerament?	SI
S'han rebut queixes d'alguna persona respecte de l'estabilitat o la seguretat del sistema de tractament darrerament?	NO
Es tracten dades especials o dades d'un nombre molt gran d'usuaris?	SI

Es calcula la probabilitat en funció del nombre de respostes afirmatives i d'acord el següent criteri:

TIPUS DE PROBABILITAT	DESCRIPCIÓ	Respostes Afirmatives
Menyspreable	És improbable que tingui lloc el risc	0-3
Limitat (Mitjà)	És possible que tingui lloc el risc.	4-8
Significatiu (Alt)	Risc molt probable en la comissió d'Infracció	8-12
Màxim (Molt Alt)	Alta probabilitat que succeeixi	Més de 12

Resultant un probabilitat d'incident LIMITADA

5.3 Risc Inicial en el tractament de dades

El risc potencial es determina com a resultat directe de l'impacte i de la probabilitat
 $RISC = IMPACTE \times PROBABILITAT$

D'acord la següent taula:

	IMPACTE			
PROBABILITAT	ACCEPTABLE	TOLERABLE	INDESITJABLE	INTOLERABLE
Despreciable (Baixa)				
Limitat (Mitjana)			x	
Significatiu (Alta)				
Màxim (Molt Alta)				

En el tractament el risc detectat és Limitat.

L'actual risc del tractament amb les mesures de seguretat existents no presenta un risc elevat que requereixi la determinació i aplicació de mesures addicionals.

El risc residual no implica alta afectació a la privacitat i intimitat de les persones que requereixi consulta a l'Autoritat Catalana de Protecció de Dades.

5.4 Mesures de seguretat

A fi de mitigar els riscos derivats de les amenaces detectades i la probabilitat es determina com a mesures necessàries per mitigar els riscos aplicables al tractament concret a partir de les definides a l'ENS (Esquema Nacional de Seguretat) el marc mínim obligatori que ha d'acomplir el servei en tant servei per mitjans electrònics lliurats a la ciutadania.

Les mesures s'han definit de forma independent del nivell de sensibilitat ENS, que ha de ser definit per l'àrea de Residus i validat per l'Ajuntament.

Part de les accions o mesures marcades estan lligades a la gestió i ubicació de la infraestructura física i requereixen determinar prèviament l'arquitectura tecnològica, si es realitzarà a la pròpia infraestructura de l'Ajuntament o a tercers ("núvol"), que no ha estat determinat a data d'aquesta avaluació.

En termes generals les mesures s'hauran d'aplicar en el primer cas per l'Ajuntament, i en el segon cas, ser preses pels tercers, garantint l'Ajuntament en qualsevol situació el compliment de la seva aplicació.

		BÀSICA	MITJANA	ALTA		
Marc organitzatiu					Control	Requisit EIPD
org.1	Categoria	Aplica	aplica	aplica	Política de seguretat	SÍ
org.2	Categoria	Aplica	aplica	aplica	Normativa de seguretat	SÍ
org.3	Categoria	Aplica	aplica	aplica	Procediments de seguretat	SÍ
org.4	Categoria	Aplica	aplica	aplica	Procés d'autorització	SI
Marc operacional					Control	
op.pl		Planificació				
op.pl.1	Categoria	Aplica	+ R1	+ R2	Anàlisi de riscos	SÍ
op.pl.2	Categoria	Aplica	+ R1	+ R1 + R2 + R3	Arquitectura de Seguretat	SÍ
op.pl.3	Categoria	Aplica	aplica	aplica	Adquisició de nous components	SÍ
op.pl.4	D	Aplica	+ R1	+ R1	Dimensionament/gestió de la capacitat	SÍ
op.pl.5	Categoria	Na	aplica	aplica	Components certificats	N/A
op.acc		Control d'accés				
op.acc.1	TA	aplica	+ R1	+ R1	Identificació	SÍ
op.acc.2	CITA	aplica	aplica	+ R1	Requisits d'accés	SÍ
op.acc.3	CITA	na	aplica	+ R1	Segregació de funcions i tasques	SÍ
op.acc.4	CITA	aplica	aplica	aplica	Procés de gestió de drets d'accés	SÍ
op.acc.5	CITA	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5	Mecanisme d'autenticació (usuaris externs)	SÍ
op.acc.6	CITA	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9	Mecanisme d'autenticació (usuaris de l'organització)	SÍ
op.exp		Explotació				
op.exp.1	Categoria	aplica	aplica	aplica	Inventari d'actius	SÍ
op.exp.2	Categoria	aplica	aplica	aplica	Configuració de seguretat	SÍ
op.exp.3	Categoria	aplica	+ R1	+ R1 + R2 + R3	Gestió de la configuració de seguretat	SÍ

op.exp.4	Categoria	aplica	+ R1	+ R1 + R2	Manteniment i actualitzacions de seguretat	Sí
op.exp.5	Categoria	na	aplica	+ R1	Gestió de canvis	Sí
op.exp.6	Categoria	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	Protecció davant de codi nociu	Sí
op.exp.7	Categoria	aplica	+ R1 + R2	+ R1 + R2 + R3	Gestió d'incidents	Sí
op.exp.8	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	Registre de l'activitat	Sí
op.exp.9	Categoria	aplica	aplica	aplica	Registre de la gestió d'incidents	Sí
op.exp.10	Categoria	aplica	+ R1	+ R1	Protecció de claus criptogràfiques	Sí
op.ext		Recursos externs				
op.ext.1	Categoria	na	aplica	aplica	Contractació i acords de nivell de servei	Sí
op.ext.2	Categoria	na	aplica	aplica	Gestió diària	Sí
op.ext.3	Categoria	na	Na	aplica	Protecció de la cadena de subministrament	N/A
op.ext.4	Categoria	na	aplica	+ R1	Interconnexió de sistemes	Sí
op.nub		Serveis al núvol				
op.nub.1	Categoria	aplica	+ R1	+ R1 + R2	Protecció de serveis al núvol	Sí
op.cont		Continuïtat del servei				
op.cont.1	D	na	aplica	aplica	Anàlisi d'impacte	Sí
op.cont.2	D	na	Na	aplica	Pla de continuïtat	N/A
op.cont.3	D	na	Na	aplica	Proves periòdiques	N/A
op.cont.4	D	na	Na	aplica	Mitjans alternatius	N/A
op.mon		Monitorització del sistema				
op.mon.1	Categoria	aplica	+ R1	+ R1 + R2	Detecció d'intrusió	Sí
op.mon.2	Categoria	aplica	+ R1 + R2	+ R1 + R2	Sistema de mètriques	Sí
op.mon.3	Categoria	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 + R6	Vigilància	Sí
Mesures de protecció					Control	
mp.if		Protecció de les instal·lacions i infraestructures				
mp.if.1	Categoria	aplica	aplica	aplica	Àrees separades i amb control d'accés	Sí
mp.if.2	Categoria	aplica	aplica	aplica	Identificació de les persones	Sí
mp.if.3	Categoria	aplica	aplica	aplica	Condicionament dels locals	Sí
mp.if.4	D	aplica	+ R1	+ R1	Energia elèctrica	Sí
mp.if.5	D	aplica	aplica	aplica	Protecció davant d'incendis	Sí
mp.if.6	D	na	aplica	aplica	Protecció davant inundacions	Sí
mp.if.7	Categoria	aplica	aplica	aplica	Registre d'entrada i sortida d'equipament	Sí
mp.per		Gestió del personal				
mp.per.1	Categoria	na	aplica	aplica	Caracterització del lloc de treball	Sí
mp.per.2	Categoria	aplica	+ R1	+ R1	Deures i obligacions	Sí
mp.per.3	Categoria	aplica	aplica	aplica	Conscienciació	Sí
mp.per.4	Categoria	aplica	aplica	aplica	Formació	Sí
mp.eq		Protecció dels equips				
mp.eq.1	Categoria	aplica	+ R1	+ R1	Lloc de treball clar	Sí
mp.eq.2	A	na	aplica	+ R1	Bloqueig de lloc de treball	Sí
mp.eq.3	Categoria	aplica	aplica	+ R1 + R2	Protecció de dispositius portàtils	Sí
mp.eq.4	C	aplica	+ R1	+ R1	Altres dispositius connectats a la xarxa	Sí

mp.com		Protecció de les comunicacions				
mp.com.1	Categoria	aplica	aplica	aplica	Perímetre segur	Sí
mp.com.2	C	aplica	+ R1	+ R1 + R2 + R3	Protecció de la confidencialitat	Sí
mp.com.3	IA	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	Protecció de la integritat i de l'autenticitat	Sí
mp.com.4	Categoria	na	+ [R1 o R2 o R3]	[R2 o R3] + R4	Separació de fluxos d'informació a la xarxa	Sí
mp.si		Protecció dels suports d'informació				
mp.si.1	C	na	aplica	aplica	Marcat de suports	Sí
mp.si.2	CI	na	aplica	+ R1 + R2	Criptografia	Sí
mp.si.3	Categoria	aplica	aplica	aplica	Custòdia	Sí
mp.si.4	Categoria	aplica	aplica	aplica	Transport	Sí
mp.si.5	C	aplica	+ R1	+ R1	Esborrat i destrucció	Sí
mp.sw		Protecció de les aplicacions informàtiques				
mp.sw.1	Categoria	na	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4	Desenvolupament d'aplicacions	Sí
mp.sw.2	Categoria	aplica	+ R1	+ R1	Acceptació i posada en servei	Sí
mp.info		Protecció de la informació				
mp.info.1	Categoria	aplica	aplica	aplica	Dades personals	Sí
mp.info.2	C	na	aplica	aplica	Qualificació de la informació	Sí
mp.info.3	IA	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4	Signatura electrònica	Sí
mp.info.4	T	na	Na	aplica	Segells de temps	N/A
mp.info.5	C	aplica	aplica	aplica	Neteja de documents	Sí
mp.info.6	D	aplica	+ R1	+ R1 + R2	Còpies de seguretat	Sí
mp.s		Protecció dels serveis				
mp.s.1	Categoria	aplica	aplica	aplica	Protecció del correu electrònic	Sí
mp.s.2	Categoria	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3	Protecció de serveis i aplicacions web	Sí
mp.s.3	Categoria	aplica	aplica	+ R1	Protecció de la navegació web	Sí
mp.s.4	D	na	aplica	+ R1	Protecció davant de denegació de servei	Sí

Fora de les mesures de l'ENS no es consideren necessàries complementàries atès el nivell de sensibilitat de les dades i l'impacte sobre la privacitat i intimitat de les persones.

6. Conclusions

El tractament de gestió de recollida selectiva i deixalleria comporta en primer lloc, un tractament de dades a gran escala, ja que es tracten dels habitants de l'Ajuntament Lliçà d'Amunt a qui es lliura els servei de recollida de residus.

El resultat d'aquesta avaluació d'impacte és el següent:

- La finalitat del tractament es realitza d'acord amb una obligació legal que habilita el tractament de dades, essent idoni i necessari.
- Les dades recollides són proporcionals a la necessitat i finalitat del tractament
- Les mesures a aplicar – amb referència l'Esquema Nacional de Seguretat (ENS) – són adients per a garantir la confidencialitat, integritat i disponibilitat de les dades d'acord el risc detectat.

Respecte a l'aplicació de les mesures de seguretat referenciades, aquestes hauran de ser exigides a les empreses licitadores en els corresponents plecs de condicions. Aquestes hauran de ser acreditades per les empreses que participin mitjançant la presentació d'un certificat emès per una entitat certificadora acreditada pel Centro Criptológico Nacional que acrediti que els sistemes d'informació relacionats amb la prestació de servei compleixen les mesures de nivell mig d'acord a l'Annex II de l'Esquema Nacional de Seguretat

L'avaluació d'impacte dona com a resultat que el nou servei a desenvolupar per la regidoria de Residus amb les mesures tècniques, organitzatives i jurídiques definides minimitzarien el risc sobre el tractament, de forma que restaria un risc residual molt baix assumible.

Sempre i quan el desplegament garanteixi els principis i mesures definides en aquesta Avaluació d'Impacte, prèvia validació del DPD, i els tècnics municipals.

La principal mesura a aplicar és la definició d'un contracte de tractament amb les empreses externes que donaran suport al procés d'implantació del nou sistema

Lliçà d'Amunt, a data de signatura de l'Informe

Joan Bernadó Casals
Assessor extern
Objetivo Tarsys, SL