1. INTRODUCTION TO PERSONAL DATA PROTECTION: KEY CONCEPTS, REGULATORY FRAMEWORK AND SCOPE

What is personal data? A person's email address? Your phone number? The identification number? An image of a person captured by a camera? A person's wallet that has been stolen? A person that has filed a complaint or claim with a City Council? All of them are personal data. An important idea is that a person's identification data is personal data, but not just the mentioned cases.

Personal data is any information relating to an identified or identifiable individual. And when is an individual identified? When a name and surname appear, a mobile phone number, an identity document number, or any other data that identifies a person.

Personal data is also information that refers to an unidentified person, but that can be identified, that is, that is identifiable. And when is a person identifiable? When an identity can be determined from any element, such as an identification code or an employee number, or a job of a single person, such as a city council secretary or auditor.

Other key concepts in the field of data protection are:

- Processing of personal data: it is any operation on personal data, whether by automated procedures or not. Therefore, it is also a treatment when a person submits a paper instance. The collection of personal data is considered its capture, but also its consultation, use or dissemination, including its destruction, so when personal data is deleted, it must be done securely. In short, a treatment is any action that is carried out with personal data.

- Data Controller: it is the person, company or entity that decides the purposes and means of the treatment. Thus, the person in charge is the one who decides to initiate the collection and processing of personal data to consider them necessary for certain purposes.

- Data Processor: is the person, company or entity that processes personal data on behalf of the controller.

- Special categories of data: these are the types of personal data to which the data protection regulations grant maximum protection. This group includes data related to ethnic or racial origin, political opinions, religion, trade union membership, genetic or biometric data, health data or data related to sexual life or sexual orientation. In relation to these special categories of data, there is a general prohibition of processing, and it is only possible to process them in very specific cases.

- Pseudonymization, which is not the same as anonymization. Pseudonymization is the process of treating data in such a way that it can no longer be attributed to a person without the use of additional information, which must be stored separately and with very strict security measures. For example, police officers are not identified by name, but by a code.

- Anonymous data: are those in which the common thread between the information and a natural person has been broken, so it is not possible to re-identify it. Data protection regulations don't apply to this, unlike pseudonymised data, to which it does.

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

The right to the protection of personal data is governed by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, also known as the General Data Protection Regulation (GDPR). The GDPR has been mandatory in all states of the European Union since May 2018.

In relation to the **scope of application**, the GDPR applies to the totally or partially automated processing of personal data; and also, to non-automated processing of personal data contained in a file or intended to be included in it. An automated data processing is one that is carried out through electronic means. This would be the case for digital documents that a person saves on their computer. In contrast, non-automated processing is done on paper.

However, this rule does not apply in the following cases:

- Activities not covered by EU Law, such as national security or foreign policy.
- Treatments carried out by an individual in the exercise of exclusively personal or domestic activities (for example, when sending a WhatsApp to a friend).
- The processing of data related to deceased persons.

Apart from these exclusions, the regulations on personal data protection do not also apply to the processing of data relating to legal persons. Therefore, a City Council, a company or a neighbourhood association does not have the Right of Personal Data protection.

From a territorial scope, the GDPR establishes that it applies to the following processing of personal data:

1. Those carried out in the activities the processor or controller established in the EU, even if the processing takes place outside the Union.
2. Those related to interested parties who are located in the EU, carried out by a non-EU processor or controller, if the processing is related to the supply of goods or services to EU stakeholders or if the processing is linked to the control of the behaviour of persons who are in the EU, whether such behaviour takes place in the Union.
3. And the last case is related to the processing of data carried out by a person not established in the EU, but in a place where the law of EU member states applies.

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

2. PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA

The principles relating to the processing of personal data are set out in Article 5 of the European Regulation and are as follows:

- The principle of lawfulness implies that personal data can only be processed if there is at least one legal basis allowing the processing. This will be addressed in the next section.
- The principle of fairness prohibits the collection of personal data by fraudulent, unfair or illegal means. An example of unfair data collection would be a user satisfaction survey on the quality of the selective collection service, which ensures that it is done anonymously, but it turns out that this is not true, and that they can link the responses to the person conducting the survey.
- The principle of transparency requires that data subjects be informed of what will be done with their data when it is collected.
- The principle of purpose limitation implies that data should be collected for specific, explicit and legitimate purposes, and that they should not be further processed in a manner incompatible with those purposes. That is, data collected for a purpose, cannot be used for anything else. However, the further processing of personal data is not considered incompatible with archiving purposes in the public interest, scientific and historical research or statistics.
- The principle of data minimisation requires that the personal data processed be adequate, relevant and limited to the purposes for which it is processed. In other words, only data that is necessary for the corresponding purpose should be collected and processed, and therefore it is necessary to avoid the processing of data that would be disproportionate.
- The principle of accuracy requires the processing of personal data that is accurate and up-to-date. It is also necessary to delete or rectify without delay personal data that is inaccurate or obsolete.
- The principle of storage limitation means that the retention of data in such a way that individuals can be identified, should only be maintained for the time necessary for the purposes pursued. After this period, they can only be kept for research, statistical or archival purposes of public interest.
- The principle of integrity and confidentiality obliges to guarantee adequate security, through the application of appropriate technical or organizational measures, in order to prevent data from being known to unauthorized persons, or from being lost. In relation to this principle, a duty of confidentiality is imposed on all staff.
- The principle of proactive responsibility or *accountability* requires the controller to be aware, diligent and proactive in relation to all processing of personal data. Therefore, the controller has the duty to ensure that all duties imposed by data protection regulations are met. And not only must comply, but must have the capacity to prove it.

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

3. LEGALITY OF DATA PROCESSING

For the processing of personal data to be lawful, it is necessary to have at least one of the legal bases established in Article 6 of the GDPR, which are detailed below.

- One of the grounds or legal bases that allow the processing of data is the consent of the interested party, which to be considered valid must be free, specific, informed and unequivocal (Article 6.1.a GDPR). Consent would be the legal basis that would legitimize the incorporation of a personalized advice model through a digital instant messaging platform (KAYT). If profiling is carried out, this consent must be explicit. Profiling is addressed in the next section.

- For the execution of a contract or the application of pre-contractual measures at the request of the interested party (Article 6.1.b GDPR). This would make it possible to process the contact details of representatives of companies contracted by a local authority or of those submitted in a tender.

- The processing is also lawful when it is necessary to comply with a legal obligation (Article 6.1.c GDPR).

- When processing is needed to protect vital interests (Article 6.1.d GDPR). It is a subsidiary legal basis, which only comes into play if it is not possible to resort to any of the other legal bases and in situations in which the person concerned is not physically or legally qualified to give consent or when data processing is necessary in humanitarian emergencies caused by natural or man-made disasters, or epidemic control.

- Another legal basis that legitimizes the treatment is when it is necessary for the fulfilment of a mission of public interest or in the exercise of official authority vested in the controller (Article 6.1.e GDPR). This is the legal basis that covers most of the data processing carried out by public sector entities, and would include the provision of the waste collection service that allows the individualization of users, the incorporation of a pay-as-you-throw scheme (PAYT) or the tasks of monitoring, control and inspection. In this last point, it is important to highlight the importance of detailing all these tasks in the corresponding municipal regulations of the local body, detailing the rules that attribute these competences to local bodies and, at the same time, specifying which agents will carry them out and in what way. This will determine the user profiles that can process the data and the specific processing they can perform.

- Processing is also considered lawful where it is necessary to satisfy the legitimate interests of the controller or a third party (Article 6.1.f GDPR). For example, a company that records customer service phone calls. However, this legal basis of legitimate interest does not apply to public administrations in the exercise of their functions.

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

4. PROFILES ELABORATION

Profiling is the processing of data to evaluate certain personal aspects of an individual; in particular, to analyse or predict aspects of that subject's personal preferences, interests, reliability, behaviour, location, or movements. For example, when you browse the Internet, certain *cookies* track what the person is browsing to determine what his preferences are and show him personalized ads.

The management of pay-as-you-throw (PAYT) waste charge can lead to the development of behavioural profiles of people using the waste collection service. Specifically, the analysis of the data generated in the provision of the service, associated with the person who uses the service through the address, allow to establish the routines or preferences of the people affected in the use of the service. That is, it allows you to evaluate certain aspects of your behaviour.

These profiles can end up having significant effects, and even legal effects if a pay-as-you-throw system is applied (for example, determining whether or not a bonus is applied) or if the data obtained is used to control how waste is deposited (for example, if poor separation collection is penalised). In such cases, these effects should be necessary to enter into or execute a contract between the data subject and a controller; which is provided for by EU or Member States law; or based on explicit consent.

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

5. DATA PROCESSING CONTRACTS

When a City Council (Data Controller) uses a company (Data Processor) for the provision of the waste collection service, from the perspective of data protection regulations, this relationship must be regulated by a contract or other legal act, such as a collaboration agreement, which must respect the minimum content determined in article 28.3 of the European Data Protection Regulation, referring, inter alia, to:

a) The object, duration, nature and purpose of the treatment.

b) The type of personal data and the categories of persons concerned.

c) The obligations and rights of the Data Controller.

d) The instructions of the Data Controller to the Data Processor.

The Data Processor may entrust certain activities to a sub-processor. To do this, a contract must be signed between them with the same data protection obligations stipulated in the initial contract signed with the Data Controller. In addition, it is essential that the Data Controller authorizes the Data Processor to contract a sub-processor.

For example, a company that manages the waste collection service (data processor), which contracts another company (sub-processor) to supply of the necessary technology for a new waste collection model, which means that the contracted company has access to the data of the users of the service.

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

6. DATA PROTECTION IMPACT ASSESSMENT

Data protection impact assessments (DPIAs), which must be carried out before processing, are not necessary for any processing of personal data, but only when there is a high risk related to the rights and freedoms of individuals, due to the nature of the processing, the scope and context, the purposes or the use of new technologies.

The European Regulation (GDPR) contains a list of treatments in which the DPIA is required:

a) when the purpose is the "systematic and exhaustive" evaluation of aspects of the person carried out automatically. For example, when profiling with legal effects, what could happen in certain cases of the use of artificial intelligence in the public sector;

b) when it comes to special categories of large-scale data, such as a hospital, or data related to criminal convictions and offences; and

c) when a large-scale systematic observation of a public access area is carried out, as would be the case of a video surveillance system in an infrastructure used daily by thousands of people.

The list of cases in which, according to the GDPR, it is necessary to carry out the AIPD to consider that they are high-risk treatments, does not have the character of a closed list, and therefore the GDPR provides that the control authorities can publish the list of the types of treatments that require a DPIA and the list of treatments in which the DPIA is not required (the lists published by the Spanish Data Protection Authority can be consulted here).

The minimum content that the DPIA should have, if necessary, is the following: a description of the processing, such as the life cycle of the data; the purpose or legal basis; the assessment of the necessity and proportionality of the processing; risk assessment and measures to minimize them; etc.

If, as a result of the impact assessment, the Data Controller continues to observe a high risk that cannot be mitigated or reduced by reasonable means in accordance with the available technology and the costs of the application, he shall consult the Control Authority before initiating such processing. The Control Authority must advise the Data Controller, but may also prohibit their processing.

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

7. OTHER OBLIGATIONS

In addition to the obligations presented so far, the GDPR imposes other obligations to the Controller.

The first of these obligations are data protection policies, for which the GDPR does not specify what their content should be. These policies are configured as one of the technical and organizational measures to be taken by the controller, which should include information on the data processing carried out by the organization, as well as its commitments in relation to data protection (for example, identification of the Controller and Data Protection Officer, how rights can be exercised, etc.).

The next obligation is the record of processing activities (RAT). The RAT has replaced the previous obligation to register files with Control Authorities, a procedure that disappeared with the GDPR. Public sector entities, such as City Councils, are obliged to have this Register.

The GDPR establishes the content of the Register (purposes of the processing, categories of data subjects and personal data, and a general description of the technical and organizational security measures, among others).

In certain cases, the obligation to have the RAT, with similar content, is also applicable to Data Processors, and the Data Controller on behalf of whom the Data Processor works, must be also identified.

The following is an explanation of Data Protection by Design and Data Protection by Default. First of all, Data Protection by Design involves taking into account all the obligations and requirements imposed by data protection regulations, from the moment a new treatment is designed. In particular, it requires the implementation of appropriate technical and organizational measures, such as pseudonymization; effectively apply data protection principles; and integrate the necessary guarantees to comply with the obligations imposed by the GDPR and to protect the rights of the concerned data subjects. For example, if a local entity decides to create an electronic channel that allows citizen participation, before implementing it, it must evaluate whether it is necessary to identify data subjects, what data is collected, how to ensure data security, how they can exercise their rights, etc.

And secondly, Data Protection by Default is the principle according to which an organisation (the data controller) ensures that only the data strictly necessary for each specific purpose of the processing are processed by default (without the intervention of the user). Thus, when a person registers on a social network, data protection by default would mean that, without having to configure anything, the profile should be private. And the other way around, if the user wants it to be public, this modification must be made by him.

The European Regulation also requires that appropriate or adequate measures be taken to ensure data security. Proper risk analysis should be performed to determine appropriate security measures.

The risk analysis should take into account the following elements: the nature of the data (e.g. whether special categories of data are processed), the number of concerned data subjects or the amount (volume of data), or the variety of processing (e.g. whether it allows profiling).

The GDPR states that security measures may consist of:

- Minimize data processing.

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

- The pseudonymization or encryption of data.
- The ability to ensure the confidentiality, integrity, availability and continuous resilience of processing systems and services, i.e. the ability to resist or recover (e.g. from a hacker attack).
- The ability to restore availability and access to personal data quickly, in the event of a physical or technical incident (e.g. with backups).
- A process for regularly verifying, evaluating, and evaluating the effectiveness of security measures. For example, this would be achieved through audits of these measures.

Another obligation is to report security breaches. This obligation implies that, in the event of any breach or incident of data security that is suffered and means a risk to the rights and freedoms of the concerned data subjects, the City Council responsible for the treatment must notify it to the competent Control Authority. This notification must be made without delay, no later than 72 hours after the time of the violation. However, if the violation is unlikely to constitute a risk to the rights and freedoms of individuals, such notification is not necessary.

In cases where the Control Authority has to be notified since the risk cannot be considered unlikely, if the Local Authority considers that the breach of security may pose a high risk to the rights and freedoms of individuals, in addition to notifying the Control Authority, the concerned data subjects should be notified, and should be offered recommendations to mitigate risks.

In any case, in the event of any type of incident that may affect the security of the data, even in cases that do not require notification to the Authority, the responsible local body must document the incident internally, noting the facts and the corrective measures adopted. This internal documentation shall be made available to the Control Authority so that it can carry out the corresponding checks.

Finally, the appointment of **a** Data Protection Officer (DPO) is mandatory in certain cases, and in any case when the Data Controller or Data Processor is an Authority or Public Body. Therefore, a City Council is required to have a DPO. However, the same DPO can be designated for several entities.

The DPO is the organization's benchmark in data protection, which, among other requirements, must have experience in this area.

The functions of the DPO are described in the data protection regulations. The most relevant are:

- It must inform and advise the Data Controller or the Data Processor, as well as its employees, on the obligations they must comply with in terms of data protection.
- It is also responsible for monitoring compliance with data protection regulations and the policies of the Data Controller or the Data Processor r, including the allocation of responsibilities, staff awareness and training, and related audits.

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

8. RIGHT TO BE INFORMED

The right to information is part of the essential core of the right to personal data protection, since it allows to exercise the power of control or disposition that subjects have over their personal data. This right that everyone has to control their personal information will only be effective if concerned subjects are informed in advance about the uses of the data, and other details that will be explained below.

In general, it is the responsibility of the controller to assert the right to information, although if the data collection is carried out by the processor, it can be set out in the contract of the controller who assumes the function to inform.

If the data is collected from the same data subject, the information must be provided at the time of collection. In these cases, the information to be provided to the concerned data subject is contained in Article 13 of the GDPR.

If, on the other hand, the data are not obtained from the concerned data subject, but from another source (e.g. another Administration), the information to be provided is contained in Article 14 of the European Data Protection Regulation, which states that it must be provided within a reasonable time, but in any case within 1 month of receiving the data, at the most.

The GDPR provides cases where it is not necessary to inform the concerned data subject, such as when the person already has the information. Or it is not necessary to report whether the data is not collected directly from the concerned data subject, but from another source, and the communication of the information is impossible or involves a disproportionate effort, or whether the collection or transmission of data is provided by EU Law or Member State law.

With regard to the content of the information to be provided, in the event that the data are obtained directly from the concerned data subject, Article 13 of the European Regulation obliges the Controller to inform at the time of collection about various issues: who is responsible and how to contact him; the contact details of the Data Protection Officer, the purposes of the processing and its legal basis; the recipients or category of recipients to whom the data may be communicated; the period of retention of the data; the possibility of exercising the rights set out below; the right to withdraw consent; the right to claim against a Control Authority; etc.

Therefore, if personal data is collected through a form, the concerned data subjects should be informed of all these details.

If the data was not obtained directly from the concerned data subject, Article 14 of the GDPR states that the concerned data subject must also be informed of the categories of data in question; and the source or origin of the personal data and, where appropriate, whether they come from publicly accessible sources, such as the Internet.

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

9. OTHER RIGHTS THAT CAN BE EXERCISED: ACCESS, RECTIFICATION, ERASURE, RESTRICT PROCESSING, DATA PORTABILITY, OBJECT AND NOT TO BE SUBJECT TO AUTOMATED DECISIONS

The GDPR recognises the following rights in relation to the processing of personal data: the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and the right not to be subject to a decision based solely on automated processing. These rights are very personal, so they can only be exercised by the owner of the data himself, although this can also be done through a legal or voluntary representative.

The deadline for replying to the request to exercise any of the rights is one month, extendable for another two months if necessary, taking into account the complexity and number of requests. If the Data Controller considers that the right exercised is not adequate, he must also respond without delay and within a maximum period of one month, indicating to the concerned data subject the reasons why the right exercised is not effective. It should also be informed of the possibility of taking appropriate measures, in particular to claim against a Control Authority.

Each of these rights is addressed below:

- Access: The purpose of this right is for anyone to know that their data is being processed by a local entity. If a person exercises this right and the Controller processes their personal data, a copy of the data being processed has to be provided, as well as other additional information, which is largely in line with the content of the right to information (purposes of processing; categories of personal data; recipients or categories of recipients; expected retention period or criteria used to determine it; etc.). The right to obtain a copy of the data cannot adversely affect the rights and freedoms of third parties.

- Rectification: through this right the person can request the modification of the data that are inaccurate, or that those that are incomplete, can be completed. When this right is exercised, the request for rectification must indicate the data to which it refers, and the rectification to be made; and must be accompanied, where appropriate, by documentation justifying the inaccuracy or incompleteness of the data that is being processed.

- Erasure or right to be forgotten: this is the right of the concerned data subject to have the personal data erasure in certain cases: when the data is no longer necessary for the purposes pursued; when the concerned data subject withdraws his or her consent; if the concerned data subject objects to the processing and other legitimate reasons for the processing do not prevail; if the data has been processed unlawfully; etc. The European Regulation lists the cases in which this right does not apply, considering that the processing is necessary to exercise the right to freedom of expression and information; to comply with a legal obligation requiring data processing, such as where archival legislation requires the

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

retention of documentation containing the data; or to carry out a task carried out in the public interest or in the exercise of official authority vested in the person responsible; etc.

- Restrict processing: allows the interested party to demand that the data can only be used in certain circumstances. In other words, it is like suspending data processing, but not erasing it. This right can be requested in the following four cases: when the Concerned data subject contests the accuracy of the personal data, during the period that allows the person responsible to verify its accuracy; when the processing is unlawful but the concerned data subject objects to the deletion of the data and, instead of erasing it, requests that its use be limited; where the controller no longer needs the data for the purposes of the processing, but the concerned data subject needs them to make, exercise or defend claims; and where the concerned data subject has objected to the processing on the basis of a particular situation, while verifying whether the legitimate reasons of the Controller prevail over those of the concerned data subject.

- Data Portability: can be exercised if the processing is carried out by automated means; and also, if it is based on the consent of the interested party or on the execution of a contract. Therefore, the right to data portability does not come into play when the processing is carried out by Public Administrations to fulfil a mission of public interest or in the exercise of public powers conferred to the controller, or in compliance with a legal obligation.

  In cases where this right applies, the concerned data subject may request the transfer of the data to another controller, or also request that the data provided to the controller be provided in a structured format.

- Object: under this right the Controller is requested to cease a certain processing of the data, and such a request is based on reasons related to the particular situation of the applicant, such as a person who may be a victim of gender violence, protected testimony, etc.

  This right may be exercised where the processing, including profiling, is based on the public interest or on the exercise of public powers vested in the Controller; in the legitimate interest pursued by the Controller or by a third party; or is carried out for scientific or historical research purposes or for statistical purposes, unless it is necessary to carry out a mission carried out for reasons of public interest. In such cases, the controller shall cease processing, unless he or she can demonstrate legitimate reasons that prevail over the interests, rights and freedoms of the data subject; or that the treatment is necessary for the formulation, exercise or defence of claims.

- Not to be subject to a decision based solely on automated processing, including profiling: in the case of Public Administrations, these decisions can be made in cases of automated processing of personal data, as if they were established in pay-as-you-throw schemes. However, this right does not exist where the automated decision is necessary to conclude or perform a contract between the concerned data subject and a Controller; where it is based on the explicit consent of the concerned data subject; or when is authorised by EU Law or Member State Law.

Except in the latter case, when the decision is authorized by an EU or Member State rule, the concerned data subject has the right to obtain human intervention from the Data Processor, to express his or her point of view and to contest the decision.

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

10. THE CONTROL AUTHORITY AND THE SYSTEM OF GUARANTEES OF THE RIGHT TO PERSONAL DATA PROTECTION

In case of breach of the duties imposed by the European Data Protection Regulation or the recognized rights to all individuals, a complaint may be filed with the competent Control Authority.

Regarding the sanctioning regime, the RGPD establishes two lists of infractions, which can be sanctioned with fines of a maximum of 10 or 20 million euros or, in the case of a company, an amount equivalent to 2% or 4%, at most, of the total annual total turnover of the previous year, and between the two options the one with the highest amount must be chosen.

However, the GDPR opens the door for Member States' legal systems to rule out the imposition of administrative fines.

On the other hand, if a person suffers damage or injury, material or immaterial (such as moral damages) as a result of a violation of the European Regulation, he or she is entitled to receive compensation from the Data Controller or Data Processor for the damages caused.

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

11. INTERNATIONAL DATA TRANSFERS

International data transfers involve the flow of personal data from the territory of a Member State to recipients established in countries outside the European Economic Area, which can only be done in the following cases:

- In specific countries, territories or sectors on which the European Commission has taken a decision recognizing that they offer an adequate level of protection.
- When adequate safeguards have been provided on the protection that the data will receive at their destination, by:
  - ✓ A binding and enforceable instrument between Public Authorities or bodies.
  - ✓ Binding corporate regulations (BCR).
  - ✓ Standard data protection clauses adopted by the European Commission or the competent Control Authority.
  - ✓ With the authorization of the Control Authority, on the basis of contractual clauses or provisions that are incorporated into binding agreements between public bodies that include enforceable rights.
  - ✓ A code of conduct that incorporates binding and enforceable commitments.
  - ✓ A certification mechanism that incorporates binding and enforceable commitments.
- When there is any of the exceptions provided in article 49 of the RGPD that allow the transfer of data without guarantees of adequate protection, for reasons of necessity linked to the interest of the owner of the data or to general interests.

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union

12. CONCLUSIONS

One of the elements to take into account when implementing a waste collection system is the personal data protection. At this point, it should be noted that local entities with competence in waste collection can process the data that is strictly necessary.

The processing of this data is legitimate in the performance of a mission of public interest or in the exercise of Public Authority. In this way, it is not necessary to obtain the consent of the concerned data subject in the provision of the waste collection service. When waste collection involves profiling that has an effect on the person using the service, such as whether a bonus is envisaged on the basis of individual contributions made, one of the following is required: the consent of the concerned data subject, the provision of an EU or Member State law for such profiling, or a contract between the data subject and a data controller.
It is also necessary to assess whether, before putting the waste collection system into operation, it is necessary to carry out a data protection impact assessment, especially if there is profiling in the established terms, as in the case of the pay-as-you-throw schemes.

Finally, it should be noted that any company or entity that provides a service to a local body within the framework of the provision of the waste collection service, which implies that it may have access to personal data, will be considered Data Processor for the treatment. In this case, the corresponding agreement or contract of Data Processor for the treatment must be signed.

The REthinkWASTE project has received funding from the LIFE Programme of the European Union.
The contents of this publication are the sole responsibility of ARC and do not necessarily reflect the opinion of the European Union