

**REGULATION OF THE INTERNAL
INFORMATION SYSTEM OF GROUP SALTO
ELECTRONICA SALTO SLU, IT SALTO SLU**

INDEX

I.	Introduction and regulatory framework	3
II.	Object	4
III.	Objective scope: infringements to be communicated through SII	4
IV.	EXCLUSIONS	7
V.	SUBJECTIVE SCOPE OF APPLICATION	7
VI.	BASIC PRINCIPLES	8
VII.	APPLICABLE REGULATIONS	9
VIII.	CALL OF DUTY	10
IX.	INTERNAL INFORMATION SYSTEM	11
X.	REQUIREMENTS OF THE INFORMATION OR COMMUNICATION/COMPLAINT	12
XI.	COMPLAINT MANAGEMENT PROTOCOL	13
XII.	PROTECTION OF THE INFORMANT/COMPLAINANT AND THE INVESTIGATED	15
XIII.	SANCTIONS	18
XIV.	TRAINING, DISSEMINATION AND AWARENESS	18
XV.	REVIEW, UPDATE AND VALIDITY	18
XVI.	CHANGE CONTROL	19

I. Introduction and regulatory framework

In accordance with Organic Law 5/2010 of 22 June, amending the Penal Code, the legal person is criminally responsible for the crimes expressly contemplated in the Law. Among its duties stands out, in accordance with LO 1/2015 of March 30, the obligation to have an organization and management model that includes the appropriate surveillance and control measures to prevent crimes or significantly reduce the risk of their commission.

GROUP SALTO (which includes ELECTRONICA SALTO SLU and IT SALTO SLU) has implemented a corporate compliance system and therefore, has approved the Criminal Risk Prevention Plan, stating an Internal Information System or Internal Complaints Channel, which is managed externally by DESCOMPLICA'T-AUDITORA URBANISTICA DE CATALUNYA S.L, and which can be accessed through the following link [Internal information system - Become uncomplicated \(descomplicat.com\)](https://descomplicat.com). In this way, we can say that SALTO's *Criminal Compliance* covers the Internal Information System, among other guarantees of regulatory compliance.

It should be noted that the outsourced management of the Whistleblowing Channel (Internal Information System after Law 2/2023) has been considered by the Attorney General's Office, in its Circular 1/2016, as a more suitable management than the one strictly internal to the company, thus guaranteeing impartiality in the management of the complaint and avoiding any type of reprisal to the informant.

This Regulation aims to develop the **Internal Information System** to adapt it to the requirements of Law 2/2023, of February 20, regulating the protection of people who report **(informants) on regulatory infringements and the fight against corruption, which transposes the European Union Directive 2019/1937, also called the Whistleblowing Directive, in matters of protection of the rights of the complainant.**

The "good work" of SALTO and compliance with the law are evidenced by the fact that (prior to the obligation) SALTO had already implemented a true *Criminal Compliance System*, managed externally by DESCOMPLICATCA'T.

Notwithstanding the foregoing, on the occasion of the entry into force of Law 2/2023, SALTO intends to adapt the previous Regulation, and that is why it approves this document, which constitutes **the second version of the Complaints Channel Management Regulation (now under the name SII Regulation)**, stating changes, with respect to the previous one, for example, in terminology – we no longer speak of whistleblower, but of informant; nor of the Whistleblowing Channel, but of the Internal Information System – and other novel aspects to be taken into account by Law 2/2023.

As a consequence of the desire to be a Group guided by ethics and the corporate values that characterize it, **anyone who knows or lives or witnesses it is invited and encouraged**

personnel a situation that may be unlawful or irregular, and is within the conduct reportable or likely to be communicated in accordance with the terms of this document, **report immediately through the channels enabled for this purpose (section III of these Regulations).**

II. Object

The **internal information system** of SALTO is an **easy and fast tool to use**, which guarantees the **confidentiality and anonymity of the informant**. This System, in addition to serving to discover and investigate possible irregularities, is an essential tool for the Code of Ethics and its values to become fully effective and to enable the continuous improvement of prevention protocols and policies, transparency rules and other internal regulations.

The purpose of these Regulations is to regulate the SALTO's Internal Information System and in particular:

- Regulate the Internal Information System according to Law 2/2023, allowing **"information or communications and complaints" to be presented**.
 - o Any reference to "complaint/information/communication in this Regulation shall be understood to cover all three terms.
- Encourage participation and communication in the company.
- Protect workers and third parties from dishonest or discriminatory acts.
- Prevent and detect regulatory breaches that occur in the company, in order to correct them, as well as acts that may constitute a criminal infringement in accordance with the principle of *"zero tolerance"* against this type of conduct in the company, as provided for in its Code of Ethics and criminal *compliance* system.
- Define the procedure for communicating and managing complaints received, as well as the guarantees and rights of the parties.
- Regulate the preferential channel **for reporting** on actions or omissions provided for in **article 2 of Law 2/2023** (those provided for in the Directive and those at national level of a criminal and administrative nature serious or very serious).

III. Objective scope: infringements to be communicated through SII

Below are the infringements that may be communicated through the SII [Internal Information System - Uncomplicate \(descomplicat.com\)](#).

Conduct susceptible to communicate/report each other	Description of behavior
Internal and external fraud	<p>-Acts that imply a benefit to the worker and a direct detriment to SALTO.</p> <p>-Fraud or scam carried out on a third party interested in SALTO.</p> <p>V. Compliance documentation, risk map Criminal, Anti-corruption Protocol</p>
Discrimination, workplace and sexual harassment	<p>- <i>Mobbing</i>, crimes against moral integrity and sexual freedom between people in the company and with third parties.</p> <p>V. Compliance documentation, risk map criminals, workplace, sexual and gender-based harassment .</p>
Acts of corruption and bribery	<p>-Give or receive from suppliers, customers, collaborators, etc., any type of preferential treatment, money, gifts or favors that may involve a modification of the conduct of both said third parties and SALTO employees or managers.</p> <p>V. Compliance documentation, risk map criminals, anti-corruption protocol.</p>
Money laundering	<p>-Infringement of the applicable regulations on the prevention of money laundering and terrorist financing.</p> <p>V. Compliance documentation, risk map Criminal.</p>
Crimes and offences against Social Security and the Public Treasury	<p>-Defraud, fraudulently benefit from a benefit, deduction or non-payment to the social security or public treasury when this constitutes a criminal or administrative offense.</p> <p>V. Compliance documentation, risk map Criminal.</p>
Infractions envelope the Rules envelope the Corporate Tax (IS)	<p>-Any conduct that violates any rule about IS.</p>

Infringements of labour law in matters of safety and health at work	-Conduct that implies a diminution of the rights and safety of workers by SALTO towards its employees. V. Compliance documentation, risk map Criminal.
Failure to comply with the regulations on the Protection of Privacy and Personal Data, and Security of Networks and Information Systems.	-Conduct infringing the applicable regulations of Personal Data Protection, security of networks and information systems, whether an internal or external infringement. V. Compliance documentation, risk map penalties, digital disconnection protocol.
Market abuse or breaches of consumer and user regulations	-Conduct tending to falsify the market or free competition. -Any conduct carried out within the Company that infringes the rights of Consumers and Users in order to correct it as soon as possible and correct the possible error. V. Compliance documentation, risk map criminals, anti-corruption protocol.
Breaches of the Code of Ethics and regulations Internal	v. compliance documentation, Code of Ethics and other compliance documentation.
Any other conduct that involves the commission of a crime	- Any conduct that implies the commission of a crime within the company or within the activity of the company. V. Compliance documentation, risk map Criminal.
Any other conduct involving the commission of a serious or very serious administrative infringement	-Any conduct carried out in the company that involves infringement of an administrative rule .
Public health	-Any conduct carried out within the company that may pose a risk to public health . V. Compliance documentation, risk map Criminal.
Damage or infringement against the environment and similar	-Any conduct carried out within the bosom of SALTO that is a clear undermining of the

	Environment or that does not comply with environmental regulations, as well as radiation protection and nuclear safety regulations. V. Compliance documentation, risk map Criminal.
Others	-This section is made available to informants to carry out their communication when they consider that none of the aforementioned behaviors includes the breach they want to report, or do not know to what conduct the Infringement to be reported.

The Regulation extends to the information/complaint of the interests contemplated in:

- Annex to Directive (EU) 2019/2937.
- Financial interests of the EU (European Public Prosecutor's Office).

Since SALTO has a criminal *compliance* system, with regard to common criminal offences between the Regulation and the risk map of said company, we refer to the latter, which establishes a detailed study of each criminal type, impact, probability in the company and control measures.

IV. Exclusions

The SALTO's Internal Information System ~~shall not apply to:~~

- Information that affects classified information.
- Obligations resulting from the protection of professional secrecy of medical and legal professionals, the duty of confidentiality of the Security Forces and Bodies in the scope of their actions, as well as the secrecy of judicial deliberations.
- Information relating to infringements in the processing of contracting procedures that contain classified information or have been declared secret or reserved.

V. Subjective scope of application

The internal information system will apply to informants working in both the private and public sectors, and who have obtained information on infringements in a work or professional context, including in any case:

- The members of SALTO (including, if any, those who have the status of public employees or employees, shareholders, participles and persons belonging to the management body, senior management or supervision of the company, including non-executive members).
- External workers (self-employed).
- Any person working for or under the direction of contractors, subcontractors and suppliers.
- Informants who communicate or publicly disclose information about infringements obtained within the framework of an employment or statutory relationship already terminated, volunteers, interns, workers in training periods regardless of whether or not they received remuneration, as well as those whose employment relationship has not yet begun, in cases where information on infringements has been obtained during the selection process or pre-contractual negotiation.

VI. Basic principles

- **Accessibility**

The SALTO Internal Information System will be accessed **clearly and easily**, through the **link enabled on Saltó's home page** – [Optimising processes \(groupsalto.com\)](https://groupsalto.com). This System will be managed by DESCOMPLICATCA'T with full confidentiality and avoiding reprisals.

- **Good faith**

Information or communication/complaint in good faith will be presumed to be one that, processed in accordance with these Regulations, reveals a series of facts or indications of irregular, unlawful or criminal appearance, and the complainant acts in the rational belief that the facts or related evidence are true.

Any complaint that aims to inform the complainant of one or more irregular, illicit or criminal acts through the DESCOMPLICATA'T page and complying with the requirements established in these Regulations is presumed in good faith.

However, bad faith information or communication/allegation is considered to be one in which the complainant is aware of the falsity of the facts narrated, or acts with manifest contempt for the truth. If it is proven that the information or communication/complaint has been made in bad faith, the protection of the informant will not act and both disciplinary and criminal measures may be applied.

- **Protection of informants**

The protection of the rights of the informant and complainant will always be guaranteed by both DESCOMPLICATA'T and SALTO. The rights of potential victims, those affected, witnesses and denounced will be guaranteed, under the same terms.

- **Confidentiality, objectivity and impartiality**

The identity of the informant will be considered confidential information. GET COMPLICATED, when receiving the information/complaints, will not reveal the identity of the informant/complainant to the Company, in order to guarantee maximum confidentiality and avoid reprisals.

Confidentiality does not imply anonymity. This means that the data of the people who make the communication may be provided to both the administrative and judicial authorities whenever they are required as a result of any judicial procedure derived from the object of the complaint. This transfer of data to administrative or judicial authorities will always be carried out in full compliance with current legislation on the protection of personal data.

Once the information or communication / complaint has been received, DESCOMPLICATA'T will guarantee the right to privacy, defense and presumption of innocence of the people subject to it. The *compliance officer* (responsible for SALTO's Internal Information System) will collaborate with DESCOMPLICATA'T to investigate the facts that are the subject of the information/complaint with objectivity, full impartiality and transparency.

VII. Applicable regulations

External regulations

- **Law 2/2023, of 20 February**, regulating the protection of persons reporting regulatory infringements and the fight against corruption, transposing Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, on the protection of persons reporting infringements of Union law.
- **Royal Decree 901/2020, of 13 October**, which regulates equality plans and their registration and amends Royal Decree 713/2010, of 28 May, on the registration and deposit of collective labour agreements and agreements.
- **Organic Law 3/2018, of 5 December**, on the Protection of Personal Data and guarantee of digital rights
- **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Internal regulations

- SALTO Code of Ethics.
- Protocol for workplace harassment, sexual harassment and harassment based on sex.
- Other internal regulations in *Criminal Compliance*.

VIII. Call of duty

Responsible for handling complaints

To preserve confidentiality and prohibit reprisals, the Internal Information System will be **managed externally by DESCOMPLICA'T**, which, after admission for processing, will instruct them together with the company's *compliance officer*, but without revealing the identity of the informants/complainants.

UNCOMPLICATE' T will have the following obligations:

- Reception and management of complaints in good faith under the principles of section IV.
- Evaluation of information or communications/complaints for processing.
- Joint investigation with the *compliance officer* of information or communications/complaints in accordance with the principles of section IV.
- Issuance of a report and a reasoned resolution with the conclusions of the investigation and report to *the compliance officer* who will send it to the management/administration bodies of the company.

Direction

Management has the obligation to ensure regulatory compliance, adopting those measures and resolutions derived from the complaint procedures. For this purpose, and in compliance with the principle of confidentiality, the Management will have restricted access to the files and they will only be communicated in the event that the *compliance officer*, by instructions of DESCOMPLICA'T, requires it in a reasoned manner; For example: in cases where it is necessary to report criminal acts to the competent authorities.

Sole administrator

The sole administrator of SALTO is responsible for the implementation of the Internal Information System, after consultation with the legal representation of the workers, and has the status of responsible for the processing of personal data in accordance with the provisions of the regulations on protection of personal data.

SALTO is responsible for the **data protection of informants and those investigated**. The personal data provided will be kept for a period of **three months** from the formulation of the complaint/communication, unless the initiation of an administrative and/or judicial procedure has been initiated or foreseeable, which requires its conservation for a longer time.

Personal data will not be communicated to third parties unless it is necessary for the processing of an internal investigation, opening of disciplinary proceedings, the adoption of disciplinary measures, or in compliance with a legal obligation they communicate to the Security Forces and Bodies and / or the Courts and Tribunals or other Authorities that are competent.

The complainant/informant may exercise the rights of access, rectification, deletion, limitation of treatment, portability and opposition, in accordance with the provisions of the General Data Protection Regulations (articles 12 and following), and in the Organic Law on Protection of Personal Data and Guarantee of Digital Rights (articles 12 and following). Any questions or queries in this matter can be consulted to the *compliance officer* and/or info@descomplicat.com.

The Compliance Officer is the person responsible for monitoring, complying with and sufficiently sufficiently the measures proposed by this Regulation, as well as processing and resolving information/complaints that may be submitted by informants. This Official will act in accordance with the guidelines established by DESCOMPLICAT, which is responsible for outsourced compliance management.

IX. Internal information system

Enabled channels

SALTO has enabled as Channels of Information / communication of infringements contemplated in Law 2/2023 and crimes susceptible to alert, the following:

- **In writing**, using the following form [Internal information system - Uncomplicate yourself \(descomplicat.com\)](#), which can be accessed from Saltó's corporate website – [Optimising processes \(groupsalto.com\)](#).
- **In person**, requesting a meeting with the person responsible for the outsourced management of the complaints channel by writing an email to info@descomplicat.com or calling the **973727615 number**.
- **By telephone**, in the **number 973727615**, which is stated on the home page of DESCOMPLICATCA'T [Protect your company with compliance - Uncomplicate yourself \(descomplicat.com\)](#). In these cases, verbal communication will be documented in the Internal Digital Information System through a complete and accurate transcription of the conversation received.

The informant will be offered the opportunity to check, rectify and accept the transcription of the message. In the event that the transcription of said verbal communication is not made, the protection of the informant and the rights that assist him will not be diminished since the communication is understood as carried out under the protection of the Law.

Once the communication has been made, it will be registered in the Digital Information System with a tracking code for each of the files, which will be received by the informants in the email indicated in the communication. With this code you can access the status of the file at any time at the following link. The Digital Information System is located in a secure database with restricted access exclusively to users

Designated.

The management of information or communications/complaints will be carried out by the **external consultancy DESCOMPLICATCA'T-AUDITORIA URBANÍSTICA DE CATALUNYA S.L. UNCOMPLICATE** yourself will carry out a

Analysis of information/complaints, **preserving the confidentiality of the complainant and avoiding reprisals.**

The Internal Information System (as long as it is integrated into *the SALTO Compliance System*) may also be used to raise queries or improvements in relation to the Criminal Risk Prevention Plan and other internal regulations.

Without prejudice to the foregoing, Law 2/2023 provides for the possibility for any natural person to report through the **external information channel of the Independent Authority for the Protection of Informants.**

X. Information or communication/complaint requirements

The information or communication/complaint will be considered to be the informant/complainant of one or more irregular, illicit or criminal acts through the web form: [Internal information system - Uncomplicate yourself \(descomplicat.com\)](https://descomplicat.com) and complying with the requirements established in these Regulations.

All reports must contain the following requirements:

1. **Identification of the complainant (unless formulated anonymously).**
 - a. **Name and surname of** the informant/complainant. The identity of the informant/complainant will be reserved by DESCOMPLICAT -which will not be provided to the company- unless the exceptional circumstances provided for in these Regulations occur (duty to notify the competent authority).
 - b. Contact email and/or telephone number.
 - c. It will also state the link with SALTO to facilitate the analysis and follow-up of the complaint.
2. **Reported irregularity: description of** the circumstances of the reported irregularity, responding to questions such as (i) what it consists of, making a clear and detailed statement of the facts, (ii) time when the event occurred or has been occurring (iii) if there are other people who can provide more information, evidentiary means where appropriate, available to the complainant (iv) area of business or company affected, (v) if there is an impact on customers, (vi) estimate, if any, of the economic damage caused.
3. **Provision of documents or evidence**, whenever possible, of the reported facts for a better evaluation and resolution of the complaint.
4. **Identification of those responsible for the irregularity**, if known.

The presentation of anonymous **communications** in the internal information system is allowed if, despite the guarantee of confidentiality, the informant chooses to remain anonymous. In case of presenting the communication/complaint anonymously, it will be convenient for the informant to state the reason for taking it into account when processing the complaint and carrying out the investigation. The fact that it is submitted anonymously may limit the processing of the file due to the impossibility of verifying the veracity of the information.

XI. Complaint management protocol

Reception

The communication/complaint may be made anonymously or nominally in the terms explained in section IV, and through the channels enabled in section III of these Regulations.

Once the communication/complaint has been made, it will be registered in the system, with a unique code. This will be recorded in the **Register of Complaints and Information of the possible infringements** contemplated in the scope of application of Law 2/2023.

The investigations carried out on the occasion of the submission of a complaint/communication will also be recorded in the **Record Book of Internal Investigations**.

Admission

Upon receipt of the communication, UNCOMPLICATE YOURSELF will check if it exposes facts or conduct that are within the reportable conduct indicated in these Regulations (section II) and if the facts could be indicatively constitutive of crime or infraction. Once this preliminary analysis has been carried out, DESCOMPLICATCA'T will decide, **within a period not exceeding ten working days from** the date of entry into the Internal Information System, it may:

- **Inadmissibility** of communication, after sharing the facts with the company's compliance officer when: (i) the facts reported do not have full plausibility; (ii) the facts reported do not constitute an infringement of the legal system included in the scope of the applicable law or within the conducts included in this Regulation; (iii) the communication is baseless or there are, in the opinion of the *compliance officer*, rational indications of having obtained this information illegally. In the latter case, whenever it could constitute a crime, the *compliance officer*, assisted by DESCOMPLICATCA'T, with the prior approval of the Management Committee, may send to the competent judicial authority the aforementioned fact that is deemed to constitute a crime; (iv) the information is a mere reproduction of a previous one previously inadmissible or duly investigated.

The inadmissibility must be communicated in a reasoned manner to the informant/complainant immediately (unless it is presented anonymously and because it has been made by call that is not returned, there is no possibility of communicating with the informant/complainant).

In the event that the information/complaint has been made in writing through the Internal Information System, the informant/complainant will receive all communications.

- **Admit** the communication/complaint for processing.

The admission **is reflected in the academic record**. The informant/complainant has real-time access to the status of their communication or complaint using the tracking code received, unless the communication/complaint has been carried out anonymously.

In the event of clearly truthful facts that constitute a crime, SALTO, with the assistance of DESCOMPLICATCA'T, will transfer the communication/report to the competent authorities immediately.

Investigation of the file

The instruction involves **the set of activities aimed at verifying the plausibility of the facts reported in the communication/report. It will be carried out by DESCOMPLICATCA'T with the collaboration of the compliance officer, who may, in turn, require the necessary information from the administrative bodies, management or departments involved.**

Rights of the investigated

The person under investigation has **the following rights**:

- **The right to know the existence of the communication/complaint and** to be informed as soon as possible that: (i) you are immersed in an investigation process, the result of a communication/complaint filed against you or your action and the facts denounced; (ii) right to lodge arguments in writing; (iii) right to the processing of your personal data; (iv) right indicated by the body responsible for management; (v) procedure for processing the complaint; (vi) right to preserve the identity of informants/complainants; (vii) Other rights that assist you.

However, the aforementioned communication may be made in the hearing process if it is considered that its contribution previously could facilitate the concealment, destruction or alteration of the means of evidence.

The instruction will include, whenever possible, an interview with the person under investigation, in which, always with regard to the presumption of innocence, he will be invited to present his version and to provide the means of proof he deems appropriate.

Resolution of the file

Once the actions have been concluded, DESCOMPLICATCA'T will issue a (non-public) report with the following information:

- Exposition of the facts related, identification code of the communication/complaint and the date of registration in the internal information system.
- Provisional legal qualification of the facts and assessment of whether they may constitute a crime or not, and whether or not it is attributable to the legal entity.
- Investigation of facts and means of evidence.
- Definitive conclusions.

Once the report has been issued, the *compliance officer* will transfer it to the sole administrator, who, with the recommendations of DESCOMPLICATA'T, will adopt one of the following decisions:

- **File of the file** to conclude that there has been no infringement in the reported conduct . The file, which will always be motivated, will be communicated to the informant and, where appropriate, to the person investigated.
- **Application of the SALTO Sanctioning Regime** to the person considered to have committed the infringement. If the act constitutes a crime, it will be immediately transferred to the competent authorities.

The period to finish the actions will be a **maximum of three** months, which may be exceeded **up to six months**, on a reasoned basis, only in cases in which the conduct was apparently constitutive of a crime.

XII. Protection of the informant/complainant and the investigated

Rights and guarantees of the informant/complainant

- Right to receive **information** prior to filing the communication/complaint, either through DESCOMPLICATCA'T, or from the company's compliance officer.
- Right to be **informed of the existence of the internal information system** (complaint channels).
- Right to file the complaint anonymously **or nominally**.
- Right to **the protection of personal data**.
- Right to file the complaint verbally **or in writing**.
- Right to **use information with a restrictive nature** (not possibility of using the information for purposes other than research).
- Right to **confidentiality** (not anonymity). Possibility of sending the information to the competent authorities if required to do so.

- Right to receive **acknowledgment of receipt within a maximum period of 7 days**. It will be issued by GET COMPLICATED automatically when filing a complaint. Therefore, although anonymity is allowed, an email must be designated in the communication/complaint in order to receive the acknowledgment of receipt.
- Right to receive **reasonable information about the status of the complaint**. It will be done automatically by DESCOMPLICATCA' T in the same terms mentioned in the previous section .
- Right to a **transparent investigation and impartiality** of DESCOMPLICAT' T and the *compliance officer*.
- Right not to **suffer reprisals** for the lawful use of the channel.

Concept of retaliation: any acts or omissions prohibited by law, or that, directly or indirectly, involve **unfavourable treatment** that places the people who suffer them at a particular disadvantage with respect to another in the work or professional context, **only because they are informants/complainants**, or because they have made a public disclosure, and provided that such acts or omissions occur during the duration of the investigation procedure or within two years of the end thereof or the date on which the public disclosure took place. The exception is the case in which such action or omission can be objectively justified in attention to a legitimate purpose and that the means to achieve that end are necessary and adequate.

Types of retaliation: for the purposes of the provisions of this Regulation and Law 2/2023, and by way of example, the following are considered **reprisals**:

- **Suspension of the employment contract, dismissal or termination of the employment or statutory relationship**, including non-renewal or early termination of a temporary employment contract once the trial period has passed.
- **Early termination or cancellation of** contracts for goods or services, imposition of any disciplinary measure, degradation or denial of promotions and any other substantial modification of working conditions.
- **Non-conversion of a temporary employment contract into a permanent one**, in the event that the worker has legitimate expectations that he would be offered permanent employment; unless these measures were carried out within the regular exercise of management power under the labour legislation or regulations of the statute of the corresponding public employee, due to accredited circumstances, facts or infractions, and beyond the presentation of the communication.
- **Damages**, including damage of a **reputational** nature, or economic loss, coercion, **intimidation, harassment or ostracism**.
- **Evaluation or negative references regarding work or professional performance**.
- Inclusion **in blacklists** or dissemination of information in a specific sectoral area, which

hinder or prevent access to employment or contracting of works or services.

- **Denial** or cancellation of a **license or permit**.
- **Denial of training**.
- **Discrimination**, or unfavorable or unfair treatment.

The person whose rights are infringed by their communication or disclosure once the period of two years has elapsed, may request the protection of the competent authority.

SALTO undertakes not to prevent or hinder the presentation of communications and complaints. Any act that includes retaliation will be null and void, and will give rise to corrective disciplinary or liability measures, and may include the corresponding compensation for damages by SALTO to the injured party.

Duties of the informant

- Act in good **faith**.
- **Provide the data, documents or any means of proof** available related to the reported facts.
- Duty of **confidentiality**. The complainant may not communicate to any body or person other than the compliance officer the identity of the accused, with the legally provided exceptions.

Protection measures

Informants/complainants will enjoy the protection measures provided for in Law 2/2023 provided that:

- They have reasonable grounds to believe that the information provided in the communication/complaint is truthful at the time of communication, even if they do not provide conclusive evidence.
- That the communication is not carried out in bad faith.
- The conduct that is the object of the communication/complaint is within the scope of Law 2/2023.
- That the complaint is made by the legitimated persons.
- In the event that the communication has been inadmissible for processing, but there is no bad faith, these protection measures will be applied.

Rights of the person affected by the communication/denounced

- Right to **know the existence of the complaint**. SALTO is obliged to report the existence of a communication/complaint.
- The right to be informed of the actions/omissions attributed to him and to be heard in any

moment.

- Right to the presumption of innocence.
- Right of access to the file, safeguarding the data of informants.
- Right to be **informed of the resolution of the** complaint/communication.

XIII. Sanctions

If after the relevant investigations it is demonstrated that there has been an action/omission constituting a crime or irregularity contemplated in these Regulations, SALTO will apply the corresponding disciplinary/sanctioning regime to the offender, or communicate the non-compliance to the competent authority, as the case may be.

XIV. Training, dissemination and awareness

These Regulations must be included among the compulsory **training** subjects of the Training Plan of SALT.

In addition, the following actions will be carried out:

- SALTO **will inform** all staff, administrators, managers and other members of the company of these Regulations, as well as to stakeholders. All SALTO workers will receive updated **compliance clause** with the communication of these Regulations and the enabling of the Internal Information System. The clause will be incorporated into all new staff additions (as an annex to the employment contract).
- Publication on Saltó's website – [Optimising processes \(groupsalto.com\)](https://groupsalto.com):
 - Criminal Risk Prevention Plan
 - Map of criminal risks
 - Code of Ethics
 - Internal Information System Management Regulations
 - Direct link to [Internal Information System - Get Complicated \(descomplicat.com\)](https://descomplicat.com)

XV. Review, update and validity

Since SALTO, through DESCOMPLICA'T is constantly monitoring *compliance*, the review of this Regulation and the rest of the documentation in *compliance* will be carried out whenever there is a

modification of the applicable regulations, must be adapted to the recommendations made by the competent authority, improvements/clarifications are made in the Internal Information System or there is any other cause that implies the need to review said documents.

In any case, it will be reviewed annually and this will be stated in the **annual audit report** issued by DESCOMPLICATCA' T.

These Regulations will be approved by the Sole Administrator on 11.4.2023, the same date on which the agreement for the appointment of *the compliance officer* as the person responsible for SII is signed. Both documents are approved after the communication made to workers (27.3.2023), and taking into account the considerations mentioned by them. In the event of numerous allegations being made, its entry into force may be postponed for a reasonable period of time without it being carried out later than 1.12.2023.

The general rule is that this Regulation will come into force the day after its approval.

For any questions or queries in the interpretation of these Regulations, it is possible to contact the *compliance officer* and responsible for the internal information system, **Blanca Rosell Cecilia** through the broSELL@esalto.es email or directly to the legal advice DESCOMPLICATCA'T (info@descomplicat.com).

XVI. CHANGE CONTROL

Document version	Approval date	Body that approves it	Effective date
1	26.10.2022	Sole administrator	27.10.2022
2	11.4.2023	Sole administrator	12.4.2023

Jaume Salto Albareda Sole
administrator GROUP
SALTO 11.4.2023