Neironix GDPR Legal Memo

Name:	Neironix
Website:	neironix.io; tokensale.neironix.io
Reference:	GDPR Legal Memo

Disclaimer: this is not an offering circular, information memorandum or any other form of offering document. GMT Legal (together with the companies of its group and their respective directors, members, officers, employees or affiliates) and the underwriters, make no representation or warranty, expressed or implied, as to the fairness, accuracy, completeness or correctness of this document, and neither the issuer nor the underwriters accept any responsibility or liability whatsoever for any loss or damage however arising from any use of this document or its contents or arising in connection with it. This document is limited to the question of analyzing and outlining the General Data Protection Regulation application to Neironix's website, as well as, including a proposed draft of documentation that should be available online. This document is limited to the information provided to the firm by Neironix and no additional investigation has been conducted to verify the veracity of such information. To the extent statements are made regarding national regulations, such statements are extrapolations based on our knowledge of EU and other Legislation, legal practice and on the principles of international harmonization of the law and on our subjective understanding of provisions and legal cases cited in the present document. There may be a need for further verification and confirmation from a specific jurisdiction professional as our subjective understanding is incomplete and our experience in international law and subjective understanding of EU and other law can strongly deviate from understanding of other EU or other professionals. The scope and basis of this document have been defined together with Neironix. Any liability towards third parties or Neironix for any statement or content of this document is explicitly excluded. It is understood and accepted that the present document does not have legal value in the EU and other and is intended for general understanding of the General Data Protection Regulation purposes only. It is understood and accepted that the GMT Legal team that has prepared the present document is not licensed to practice law in the EU and other and that no warranties or representations have been made to this regard. GMT Legal services team may consist of jurists that may be educated and may be trained in EU, other and international law, and may consist of jurists that may be licensed to practice law in any jurisdictions in Europe, Latin America or Asia. GMT Legal professional liability insurance does not apply to any statement or content of this document. Please note that where a legal provision or a rule has been amended, edited or replaced by another and therefore there seems to be a legal freedom to operate the business activities, this does not exclude that other rules may exist pertaining to the regulation of the business activities.

Confidentiality: This document is strictly private, confidential and personal to its recipients and should not be copied, distributed or reproduced in whole or in part, nor passed to any third party.

EU Regulation:

The General Data Protection Regulation ("GDPR"), Regulation (EU) 2016/679, has entered into force on May 25th, 2018, replacing the Data Protection Directive 95/46/EC. Different than a Directive, a Regulation is directly applicable in all EU Member States. Its main purpose is to enforce data protection and to enhance consumer confidence in the single digital marketplace.

Regardless of where your organization is located, if you collect data of natural persons resident in any EU Member State you will be subject to the GDPR. The periodicity of the data collection and the kind of information you collect will play a key role on the relevant regulations to your organization.

More specifically, the GDPR applies to the processing of personal data by automated means and to the processing of personal data, which forms or intends to form part of a filing system. The GDPR only applies when the data subjects are EU citizens or residents where the processing activities are related to the offering of goods or services or the monitoring of their behavior.

The GDPR also establishes the principles that must be followed when processing data, in summary: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and, accountability.

The conditions for consent are an important part of the GDPR, when integrating a consent-based system of data processing, it is important to be able to demonstrate that the data subject has declared his or her consent univocally and the request shall be made in a clear and distinguishable manner, as well as, intelligible, easily accessible form, and using clear and plain language. It is also important to allow the data subject to withdraw consent at any time in an easy and accessible manner.

The data subjects have certain rights in respect of the data that the controller and processor hold and process, among those rights; the data subjects have the right to request information to the controller or processor regarding their data. This request shall be replied for free and without delay and maximum within one month of receipt of the request.

Additionally, it is necessary to maintain records of the processing activities, containing the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations; and information regarding transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and the documentation of suitable safeguards.

The GDPR also establishes that it is necessary to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and, a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Information that must be provided to the data subject:

- Contact details of the controller or representative;
- Contact details of the data protection officer;
- Purpose of processing;
- Legal basis for processing;
- Where the processing is based;
- If the data will be transferred to a third country, and if so, the safeguards in place;
- Period for which the data will be stored;
- Information regarding the availability to request access to the data, rectification or erasure;
- Information regarding the possibility to withdraw consent;
- Information regarding the right to lodge a complaint; and,
- Information of the existence of automated decision-making, including profiling.

Notification of Breach:

Under the GDPR, it is necessary to notify the supervisory authority within 72 hours after having become aware of a personal data breach. A supervisory authority is competent within their territory, therefore, if the breach compromises the data of several territories of the EU, it will be important to notify each supervisory authority within the 72 hours period.

The notification shall include a description of the nature of the personal data breach; the name and contact details of the data protection officer; a description of the possible consequences of the breach; a description of the measures taken or proposed to be taken by the controller to address the breach.

Additionally, it is necessary to notify the data subjects of the breach without undue delay, with a description - in clear and plain language - the nature of the personal data breach and should contain description of the possible consequences of the breach; a description of the measures taken or proposed to be taken by the controller to address the breach.

Designation of a Representative:

Where the organization that is collecting the data is located outside the EU, it is necessary to appoint a representative to act on behalf of the controller or the processor and may be addressed by any supervisory authority and the data subjects.

Designation of a Data Protection Officer:

It is necessary to appoint a Data Protection Officer when the processing of data requires regular and systematic monitoring of the data subjects on a large scale or when processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation; or personal data relating to criminal convictions.

The Data Protection Officer must have expert knowledge of data protection law and practices and fulfill the tasks of: informing and advising the controller and processor and the employees who carry out the processing of data about their obligations under the GDPR; monitoring the compliance with the GDPR; providing advice regarding the data protection impact assessment; cooperating with the supervisory authority; and acting as a point of contact for the supervisory authority.

Transfer of Data to Countries Outside of the EU:

Any transfer of Personal Data of EU Data Subjects must follow the GDPR and the General Principles for International Data Transfers. In general, the GDPR requires that the country outside the EU that will receive the Personal Data ensures an adequate level of protection equivalent to the requirements of the EU and the GDPR. The European Commission has the responsibility to issue an adequacy decision regarding each country to determine the level of protection that each country offers, if there is no such decision, the controller or processor shall provide appropriate safeguards by a legally binding and enforceable instrument between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the Commission; standard data protection clauses adopted by a supervisory authority and approved by the Commission; approved code of conduct; approved certification mechanism.

Administrative Fines under the GDPR:

Concept	Fine
Infringement to the conditions applicable to child's consent in relation to information society services.	Up to 10,000,000 EUR or 2% of the total annual turnover of the preceding financial year
Infringement of cases where data processing does not require identification	Up to 10,000,000 EUR or 2% of the total annual turnover of the preceding financial year
Non-implementation of the appropriate technical and organizational measures	Up to 10,000,000 EUR or 2% of the total annual turnover of the preceding financial year
Infringement of the data protection officer tasks	Up to 10,000,000 EUR or 2% of the total annual turnover of the preceding financial year
Infringement of certification conditions	Up to 10,000,000 EUR or 2% of the total annual turnover of the preceding financial year
Infringement of the obligations of monitoring	Up to 10,000,000 EUR or 2% of the total annual turnover of the preceding financial year
Infringement of the basic principles of processing, including the conditions for consent	Up to 20,000,000 EUR or 4% of the total annual turnover of the preceding financial year.
Infringement of the data subject's rights	Up to 20,000,000 EUR or 4% of the total annual turnover of the preceding financial year.
Infringement of the conditions for transfer of data to countries outside the EU	Up to 20,000,000 EUR or 4% of the total annual turnover of the preceding financial year.

Non-compliance with a Member State legislation	Up to 20,000,000 EUR or 4% of the total annual turnover of the preceding financial year.
Non-compliance with an order of the Supervisory Authority	Up to 20,000,000 EUR or 4% of the total annual turnover of the preceding financial year.

Additionally, other penalties may apply in accordance with each Member State's rules; this would have to be analyzed on a case by case basis.

Important Definitions according the GDPR:

- Personal Data: means any information relating to an identified or identifiable natural person. It includes: name, identification number, location data, online identifier or other indirect factors such as physical, physiological, genetic, mental, economic, cultural or social identity.
- Data Subject: the natural person of whom the data is being collected.
- Processing: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data.
- Controller: natural or legal person that determines the purposes and means of the processing of personal data.
- Processor: natural or legal person that processes personal data on behalf of the controller.
- Consent of the data subject: freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by statement or clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- Representative: natural or legal person established in the EU and designated by the controller or processor in writing to be addressed by the supervisory authorities and the data subjects, on all issues related to the processing of personal data and ensuring compliance with the GDPR.

Compliance:

In the case of Neironix, it is understood that Neironix is both a Controller and a Processor of data, and therefore, should comply with various requirements that the GDPR sets in order to maintain certain level of protection and information for the users.

Therefore, we have prepared specific documentation that we recommend Neironix to make available online. This documentation involves information regarding the use of cookies and privacy policy.

Cookie Notice:

Добавлено примечание ([ДП1]): This is for Tokensale.neironix.io

As user of our website (tokensale.neironix.io), you are informed that we use cookies and similar technologies. Cookies are small data files installed in the user's device that makes it possible to store information about your page activities. More specifically, cookies enable our website to access, among other data, information regarding the last date and time you have viewed our website; the content layout you have selected when first visited our website; security factors involved in controlling access to restricted areas. You have the option to prevent the generation of cookies by selecting the relevant option in your browser.

Cookies enable our website, to store and retain information about your browsing habits or devices and, depending on the information contained in the devises and the activities performed on them, they can be used to recognize you as a user of our website.

Our website uses the following third-party cookies:

Name	Origin	Purpose	Duration	Type
ref_code	tokensale.neironix.io	Preserves referral code	One week	HTTP Cookie
_language	tokensale.neironix.io	Remembers the user's selected language version of a website:	One month:	HTTP Cookie
advanced-ico	tokensale.neironix.io	Preserves users states across page requests.	Session	HTTP Cookie
_identity-ico	tokensale.neironix.io	Identifies the user and allows authentication to the server	One month	HTTP Cookie
_csrf-ico	tokensale.neironix.io	Used to prevent cross-site request forgery	Session	HTTP Cookie
preInvestModal	tokensale.neironix.io	Defines whether modal; window is shown	Session	
_gat_gtag_UA_111274536_1	www.google-analytics.com/	Used to send data to Google Analytics about the visitor's device and behaviour. Tracks the visitor across devices and marketing channels.	One day	
_ga	www.google-analytics.com/	Used to send data to Google Analytics about the visitor's device and behaviour. Tracks the visitor across devices and marketing channels.	Two Years	
_gid	www.google-analytics.com/	Used to send data to Google Analytics about the visitor's device and behaviour. Tracks the	One day	

		visitor across devices and marketing channels.		
_ym_isad	mc.yandex.ru	Used to send data to Yandex.Metrica about the visitor's device and behaviour. Tracks the visitor across devices and marketing channels.	20 hours	
_ym_d	mc.yandex.ru	Used to send data to Yandex.Metrica about the visitor's device and behaviour. Tracks the visitor across devices and marketing channels.	One day	
_ym_uid	mc.yandex.ru	Used to send data to Yandex.Metrica about the visitor's device and behaviour. Tracks the visitor across devices and marketing channels.	One day	

As our user, you can customize the installation of cookies during our website settings process and you are hereby aware that disabling cookies and similar technology can affect the normal use of our website and of the services our website provides.

To disable cookies:

Safari: Preferences -> Privacy -> Security

Chrome: More -> Settings (or Preferences on a Mac) -> Advanced -> Privacy -> Content settings

Firefox: Options -> Privacy & Security ->Display cookies

Internet Explorer: Tools -> Internet Options -> Privacy -> Settings

Cookie Notice:

Добавлено примечание ([ДП2]): This is for neironix.io

As user of our website (neironix.io), you are informed that we use cookies and similar technologies. Cookies are small data files installed in the user's device that makes it possible to store information about your page activities. More specifically, cookies enable our website to access, among other data, information regarding the last date and time you have viewed our website; the content layout you have selected when first visited our website; security factors involved in controlling access to restricted areas. You have the option to prevent the generation of cookies by selecting the relevant option in your browser.

Cookies enable our website, to store and retain information about your browsing habits or devices and, depending on the information contained in the devises and the activities performed on them, they can be used to recognize you as a user of our website.

Our website uses the following third-party cookies:

Name	Origin	Purpose	Duration	Type
ref_code:	neironix.io:	Preserves referral code	One week	HTTP Cookie
_language	neironix.io	Remembers the user's selected language version of a website:	One month:	HTTP Cookie
advanced-frontend	neironix.io	Preserves users states across page requests.	Session	HTTP Cookie
mainPageOrder	neironix.io	Preserves block sorts on main page.	One month	HTTP Cookie
_identity-frontend	neironix.io	Identifies the user and allows authentication to the server	One month	HTTP Cookie
_csrf-frontend	neironix.io	Used to prevent cross-site request forgery	Session	HTTP Cookie
tg-notify	neironix.io	Defines whether modal; window is shown	One day	
_gat_gtag_UA_111274536_1	www.google-analytics.com/	Used to send data to Google Analytics about the visitor's device and behaviour. Tracks the visitor across devices and marketing channels.	One day	
_ga	www.google-analytics.com/	Used to send data to Google Analytics about the visitor's device and behaviour. Tracks the	Two Years	

		visitor across devices and marketing channels.		
_gid	www.google-analytics.com/	Used to send data to Google Analytics about the visitor's device and behaviour. Tracks the visitor across devices and marketing channels.	One day	
_ym_isad	mc.yandex.ru	Used to send data to Yandex.Metrica about the visitor's device and behaviour. Tracks the visitor across devices and marketing channels.	20 hours	
_ym_d	mc.yandex.ru	Used to send data to Yandex.Metrica about the visitor's device and behaviour. Tracks the visitor across devices and marketing channels.	One day	
_ym_uid	mc.yandex.ru	Used to send data to Yandex.Metrica about the visitor's device and behaviour. Tracks the visitor across devices and marketing channels.	One day	

As our user, you can customize the installation of cookies during our website settings process and you are hereby aware that disabling cookies and similar technology can affect the normal use of our website and of the services our website provides.

To disable cookies:

Safari: Preferences -> Privacy -> Security

Chrome: More -> Settings (or Preferences on a Mac) -> Advanced -> Privacy -> Content settings

Firefox: Options -> Privacy & Security ->Display cookies

Internet Explorer: Tools -> Internet Options -> Privacy -> Settings

Privacy Policy:

1. Introduction
2. The data Neironix collects about you
3. How is your personal data collected
4. How we use your personal data
5. Why we use your personal data
6. Disclosures of your personal data
7. International transfers
8. Data security
9. Data retention
10. Your rights

1. Introduction:

Neironix OU, a Company incorporated in Estonia at Tallin, Estonia, Roosinkrantsi 2-K408 (hereinafter "Neironix") provides access to neironix.io website domain name and any other subdomain names (e.g. tokensale.neironix.io) (hereinafter "Website"), content and such services that from time to time require the collection of certain information from you (Neironix, throughout this privacy policy, referred as "Neironix", "we", "us", or "our"). This privacy policy is issued on behalf of Neironix as the controller and processor of the data collected through the use of Website.

Neironix is committed to privacy, data protection, the responsible use of information and the need to safeguard the privacy of its clients, users, partners and visitors of Website at all times. Additionally, Neironix is committed to maintaining compliance with the General Data Protection Regulation (GDPR) and the Personal Data Protection Act of the Republic of Estonia. Neironix ensures that the data you supply is processed fairly and lawfully, and with skill and care. Neironix takes this responsibility in respect of your personal data extremely seriously.

This privacy policy is a statement that sets out our commitment, the conditions, and forms under which we collect and process information, including personal and identifiable information through the use of our website, our services or any other relationship we maintain with you, including any information that you may provide us through this website when you contact us for any reason such as joining our marketing list, registering for an event, downloading content, requesting information about our services, sending us a request for a proposal or quote, or filling in a survey. Our website is not intended for children and we do not knowingly collect data relating to children through this website.

Should you have any questions regarding the handling of your data and this privacy policy, including any requests to exercise your legal rights please contact us at support@neironix.io

You have the right to make a complaint at any time to the supervisory authority of your jurisdiction. We would, however, appreciate if you would allow us to deal with your concerns before you approach the relevant supervisory authority.

Our website may include links to third-party websites, plug-ins and applications as well as embedded content such as videos, leaflets and other related content. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

2. The data Neironix collects about you:

Personal data, or personal information, means any information that identifies an individual. It does not include data where the identity has been removed. We may collect, use, store and transfer different kinds of personal data about you, such as: email address, first name, last name, passport photo, date of birth, nationality, phone number, address, utility bill, password of your registered account with us (hashed), ETH wallet address, investor status, place and time of your session at Website, and any other information we consider relevant to the provision of our services and the adequate use of our website.

We do not share certain identifiable information with third parties for the purposes of identity verification in compliance with Customer Due Diligence (CDD), Know Your Client (KYC), and Anti Money Laundering (AML) policies and regulations we handle compliance internally. We may also collect, use and share "Aggregated Data" such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered identifiable information in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data that will be used in accordance with this privacy policy. We do not collect any Special Categories of Personal Data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

3. How is your personal data collected?

We use different methods to collect data from and about you including through direct and automated technologies interactions. You may give us your Identity and Contact Data by filling in forms or by corresponding with us on the Website. This includes personal data you provide when you subscribe to our service, events or publications; request marketing to be sent to you; send us information about a request for proposal; contact us in relation to a business, media or supplier enquiry; or give us some feedback.

As you interact with our Website, we may automatically collect Technical Data about your equipment through automated technologies or interactions, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. Please see our cookie policy for further details.

4. How we use your personal data?

We will only use your personal data when the law allows us to use it. Most commonly, we will use your personal data where we need to perform the contract we are about to enter into or have entered into with you; where it is necessary for our legitimate interests and your interests and fundamental rights do not override those interests; where we need to comply with a legal or regulatory obligation.

You have the right to opt out at any time by contacting us and we will stop collecting and/or processing your data and we will proceed to delete it completely from our systems.

5. Why we use your personal data?

We use your personal data mainly to comply with CDD, KYC and AML policies and applicable regulations. It is a core part of our service to maintain the highest degree of diligence and reputation in front of you, other users and clients, business partners, and third party service providers.

Furthermore, we use your personal data to manage our relationship with you (e.g. to inform you about changes on our terms and/or privacy policy), this use of personal data fall within the lawful basis for collection of personal data (i.e., performance of a contract with you; necessary to comply with a legal obligation; necessary for our legitimate interest). We may also use your personal data to protect our

business and our website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data) forming part of our legitimate interest.

We will only use your personal data for the purposes that we collected it for, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us. Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

6. International Transfers:

We share your personal data with our head office and our business partners or service providers when this is absolutely necessary. This will involve transferring your data outside the European Economic Area (EEA).

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented: a) where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. For further details, see European Commission: Model Contracts for the transfer of personal data to third countries (https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en). b) where we use providers based in the US, we may transfer data to them either based on Model Contracts, or if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US. For further details, see European Commission: EU-US Privacy Shield (https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en).

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

7. Data security:

We have a SSL certificate and "Two Factor Authentication" (2FA) and authorization by phone mechanism in our website and we have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal data to some employees, agents, contractors and other third parties who do not require processing your personal data. Further, we use pseudonymisation and encryption of your personal data to secure its storage within our systems.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

9. Data retention:

We will only retain your personal data for as long as it is necessary to fulfill the purposes we collected it for. Including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period of personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data. The purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Under the law, we keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for six years after they cease being customers for tax purposes. In some circumstances we may anonymize your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

10. Your rights:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of your personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Object to processing of your data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances. We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response. We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated. We will, nevertheless, in all cases confirm a reception of your request within 72 hours from the time we receive your request.