



Data Protection Policy





INTRODUCTION

As an expression of social responsibility, the AndSoft Group commits to comply with the legislation on personal data protection and to that provided by the European Data Protection Regulation (EDPR) with entry into force on the 25th of May of 2018.

Data protection is the core of a business relationship based on trust and therefore an integral part of the AndSoft Group' policies. For this reason, by means of the present document we wish to express our efforts to protect the privacy and confidentiality of the personal data in connection with the provision of our activities¹, whether it is personal data belonging to clients, suppliers or our own workers.

In order to be able to provide our services, it is possible that certain information, included Personal Data, has to be shared with the companies of the different collaborators of ANDSOFT (ex. Hosting companies, accounting/financial management). If that were the case the client or supplier would be duly informed.

¹ Development of a TMS software for transportation and logistics companies

1. IDENTIFICATION OF THE DATA CONTROLLER AND CONTACT

ANDSOFT EUROPE SARL, with headquarters situated at 19 Rue de Bitbourg, L-1273, Luxemburg - Luxemburg (from this point on **AndSoft**) with VAT number LU 26 252 867 is accountable for the treatment of Personal Data received in relation to the services provided to its clients.

In certain cases, in order to be able to provide the service, AndSoft and its client/supplier may have agreed to handing over data control to AndSoft, in this case the obligations to be followed will be established in a contract signed between AndSoft and the client.

2. PERSONAL DATA OBJECT OF PROCESSING

As a direct consequence of our activities, we can collect and process the following personal data:

Identification Data → name and surnames, contact details (email, telephone number), sex, employer, work position

3. HOW DO WE OBTAIN PERSONAL DATA?

Depending on the service provided to the client, ANDSOFT can collect personal data from different sources such as:

- Email
- Corporative Web (www.andsoft.com)
- Meetings with clients

4. PURPOSE OF THE PROCESSING

In this section we will establish for which purpose we control or use the Personal Data, and we will identify each process with its corresponding legal basis.

These "legal basis" are established in the General Rules of Data Protection (GRDP) and allow the companies to process Personal Data only when said process is specified in an article of the Regulations.

SUBJECTS OF DATA PROCESS	PURPOSE	LEGAL BASIS	ADDITIONAL INFO
-----------------------------	---------	-------------	-----------------

Clients (or potential clients)	- Provision of service be it precontractual or contractual	Art. 6.1.b) GRD	
Workers	- Making of pay slips and wages payment - Social Security - Any other derived from a strictly professional relationship	Art. 6.1.c) GRD	
Suppliers	- Upkeep of the contractual relationship (between the parties and third parties) - Diffusing information, commercialising, (always duly identified as such), communication and notification	Art. 6.1.b) GRD	
Candidates that send their CV	Becoming a part of the process of staff selection, employment agency and recruitment being carried out.	Art. 6.1.a)	Consent will be requested via email to all the candidates that send their CV. 12 months after reception of the CV it will be deleted.
User Data in fairs/congresses	Subsequent contact with the person concerned to gather further information about the company / provided services	Art. 6.1.a)	A consent check box for data processing will be included in the data form.

Internet browsing data (IP, cookies)	Provision of services of informative nature requested by the Users	Art. 6.1.a)	Consent will be requested to enter the homepage of the Website. Go to “cookies processing”.
---	--	-------------	--

Under no context does AndSoft process data that includes data relative to ethnical or racial origin, religious, political or philosophical ideologies, union affiliation, genetic or biometric data, health data, data of sexual orientation or any other data that goes against the rights and freedom of people.

HOW LONG TO WE KEEP THE DATA?

Personal Data that is subject to a contractual relationship is stored, at least, until the end of the contractual relationship. Once this relationship is terminated the data will be deleted or cancelled, if the person concerned has no pending obligation, except if the data needs to be stored for any of the following reasons:

- Legal obligation → storage of invoices, accountancy entries, money laundering, etc.
- Legitimate interest → This is the case of workers, ANDSOFT must store a historic record of the staff that have worked for the company. In any case all data will not be stored, only the data necessary to said record.

In the event that none of the above-mentioned circumstances are met, the data will be deleted. In the case of CVs, under no context will they be kept for more than 12 months after reception (and non-utilisation) or after the selection process has ended.

In the possible case of data compilation for commercial purposes during a fair or congress, if the party concerned does not request that the data be deleted, it will be stored and used for future commercial activities.

Given that a storage period has been established for each category of data, we must also establish the deleting mechanism of the data once it has reach the end of its storage period and all supports.

5. CONSENT OF THE INTERESTED PARTY

As a result of the enforcement the new GRDP, AndSoft will only process data of the concerned parties that have given their previous consent, unless said processing stems from a legal basis (as mentioned in point 4 – purpose of processing).

In the case that the consent of the concerned party is necessary (ex. when the concerned party sends a CV by email or when browsing the website for the first time), an automated email will be sent in which the person concerned will have to give consent for the processing the data, via given instructions.

When requesting said consent, the person concerned will be informed of his rights, in accordance with section 7.1.2 of the present document. The declaration of consent will always be registered in the system to the effect that the person concerned can withdraw it at any time (except in cases where it is necessary to process the person' concerned data under the cases of the art. 6 of the EDPR - request of the processing).

In the case in which the data is given for first time via phone, the concerned party will have to give his consent via email in the case that the relationship is continued at posteriori and the data will be processed.

6. USE OF COOKIES

Natural persons can be associated to online identifiers, such an internet protocol address (IP address), cookies and other identifiers. This could leave a trace that can, especially if combined with unique identifiers and others received by servers, be used to create profiles of natural persons and identify them.

From the moment cookies can identify a person it is considered personal data.

The ANDSOFT website (www.andsoft.com) uses sessions and permanent cookies, and duly informs the users from the first access to the website, that they must give their consent to use cookies.

WHAT COOKIES DO WE USE AND WHAT FOR?

The AndSoft website uses the following cookies:

TYPE OF COOKIE	PURPOSE
----------------	---------

<p>Analytical Cookies</p>	<p>Our website uses Google Analytics to analyse and optimise the functionalities of our website. More specifically, it is used whilst a user is browsing during a session, and to remember chosen selections and visited pages on our website, etc.</p> <p>It obtains general information on the accesses of the user to our website (not of their content) to subsequently compile the added information from those accesses to draw up statistics.</p> <p>Google Analytics is a web analytical service loaned by Google, Inc, a company belonging the Delaware group with headquarters at 1600 Amphitheatre Parkway, Mountain View (California), CA 94043, USA ("Google").</p> <p>Google Analytics use cookies to analyse how a user uses a website. The information generated by the cookie on the use of the website (including the IP) will be directly transmitted and archived by Google in their US servers.</p> <p>Google will use this information to keep track of the use of the website, compiling reports of the activity of the website and offering other services related to the activity of the website and internet use. Google will be able to forward this information to third parties when required by the law, or when said third parties process the information for Google. Google will not associate the IP address with no other data they possess.</p>
<p>Personalisation Cookies</p>	<p>These cookies enable the user to specify or personalise some of the characteristics of the general options of the website, such as, the language, regional configuration, type of browser.</p>
<p>Technical Cookies</p>	<p>Technical cookies are essential and strictly necessary for the correct functioning of the website and the use of the different options and services available.</p> <p>For example, they are used to keep a session active, for response time management, for performance or option validation, as security items, to share content with social media, etc.</p>

You can decline the processing of data or information by declining the use of cookies by appropriately configuring your browser, but if you choose to do this you may not be able to have access to the full functionalities of the website.

Apart from declining the use of cookies you can also install in your browser the option to disable Google Analytics, that stops Google Analytics from compiling information on visits to other websites.

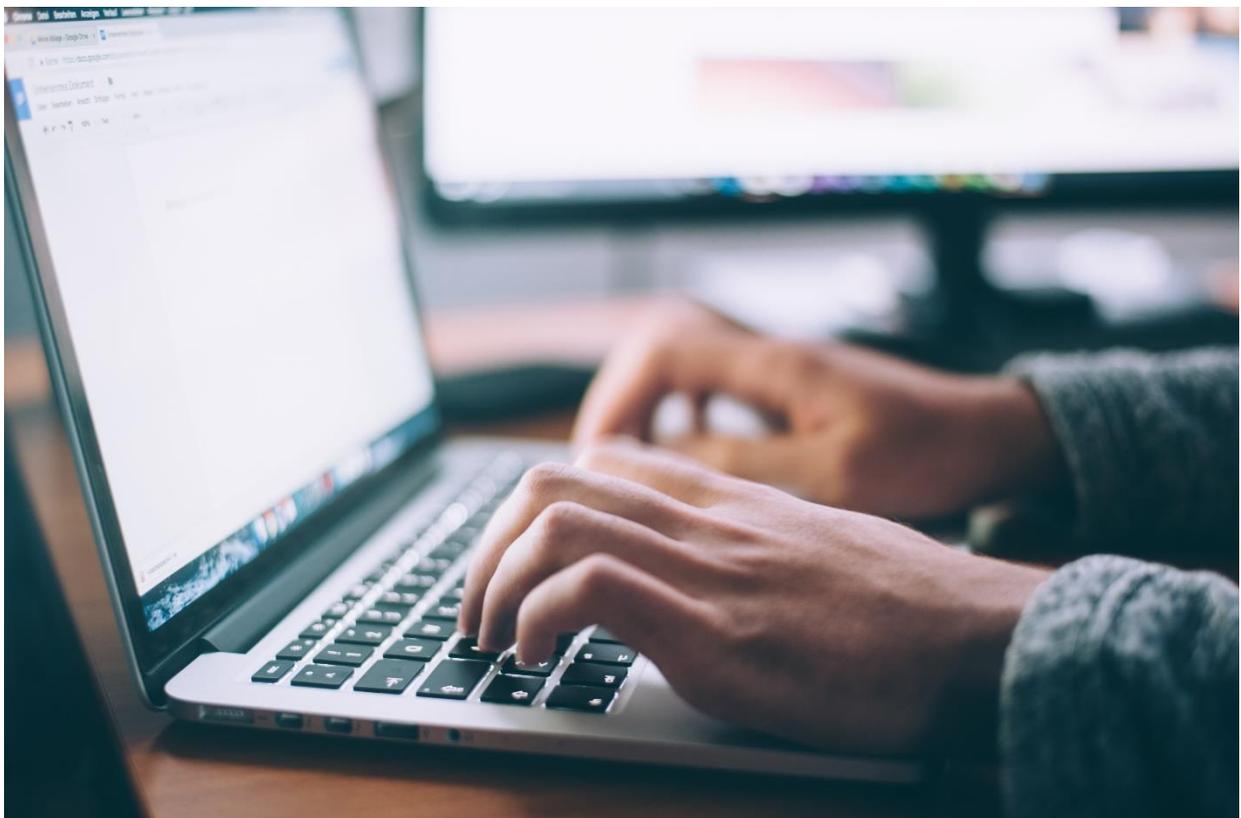
WHAT HAPPENS IF I DON'T USE COOKIES?

To comply with current legislation, we must ask for the user's permission to manage cookies. If the user decides not to authorise their use, by declining their use, we would only use technical cookies because these are essential to browse the website. In this case we would not store any cookies.

The user must consider that by declining or deleting the cookies from the browser of the website, preferences will not be remembered, some characteristic of the page will not be available and each time the user comes back to the website permission to use cookies will be asked. If the user still wants to change the access configuration to the website, he must know that it is possible to delete the cookies or stop this information from being stocked on his computer by changing the configuration parameters of his browser. Internet Explorer, Firefox, Google Chrome or Safari. These search engines are object to actualisations or modifications, so we cannot guarantee that they will completely adapt to the version of your browser.

It is also possible that the user uses a search engine not contemplated in those links such as Konqueror, Arora, Flock, etc. To avoid conflicting functioning, you can go to the options of your search engine, in the options menu go to the “Private” option (please go to the search engine help guide for further information).

By adopting this policy, ANDSOFT, proves its commitment to the existing legislation in the use of cookies, giving the user the necessary information to understand what type of cookies we use and why we use them. By doing so we wish to be clear in the use of the data processed whilst browsing our website. This policy is periodically revised in order to establish its validity and there for cannot be changed. We recommend you visit our page regularly, so we can inform you of any updates on the matter. Where can I get more information? If you have any further question on how we use cookies, please send us an email at info@andsoft.com. If you need more information on cookies guidelines, please go to the following link <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0136&from=EN>



7. GENERAL INFORMATION

Article 5.1f of the EDPR states the need to establish adequate security guaranties against the non-authorized or illicit processing of data, against the loss of personal data, destruction or accidental damage of personal data. Taking this into consideration, ANDSOFT, has conducted a study on possible risks that processing data entails, revising and updating our technical and organisational means to guarantee the integrity and confidentiality of personal data in accordance with the law established on the 25th of May 2018.

Additionally, according to the principle of accountability established in the EDPR our will and commitment is to convey that said measures are effectively implemented in the following ways:

7.1. ORGANISATIONAL MEASURES

All ANDSOFT staff with access to personal data must know his or her obligations when processing personal data, being informed of said obligations by an official statement issued by the company. The minimum information given to the staff is the following:

7.1.1. DUTY OF CONFIDENTIALITY AND SECRECY

- Prevent the access to personal data from non-authorized personal.
- For that purpose, exposing personal data to third parties will be avoided (disregarded electronic screens, paper documentation left disregarded in public spaces, technical supports with personal data, ect.).

When a staff member leaves his/her working space, the screen must be locked, or the session closed.

- Paper documents and technical supports that contain personal data will be stored in a safe place (cupboards, or shelves with restricted access) 24 hours a day. The last staff member to leave the office will make sure the main door is closed and lock by key.
- No document or technical support containing personal data (CD, pen drives, hard disc, etc.) will be discarded without guaranteeing its destruction.

All the ANDSOFT headquarters dispose of a minimum of one paper shredder. Additionally, each physical point has at its disposal an associated company for the destruction of technical supports. Each of these companies has signed the corresponding contract relating to the handling of this process.

- In no case will personal data or any general personal information be forwarded to third parties: special attention will be given so no personal data is divulged during telephone conversations, correspondence, emails, etc.

- The duty of secrecy and confidentiality is ongoing, even when the professional relationship with the company is terminated.

7.1.2. RIGHTS OF THE DATA HOLDERS

All our workers will be duly informed about the procedure to follow to comply with the rights of those concerned, clearly defining the mechanism whereby they can exercise those rights (electronic means, reference to the Chief Data Protection is there where one, address, ect.) considering the following:

- The holders of personal data (those concerned) will be able to exercise their right to accessibility, rectification, suppressibility, opposition and portability by sending us an email to info@andsoft.com, and duly justifying their identity with a copy of an official identification document (ID, passport or driving license). The person responsible of the process will have to give an answer to the person concerned within the briefest of delays.

For **access rights** the persons concerned will be given a list of the personal data at the disposal of the person in charge of the process and the purpose for which they have been chosen, the ID of the recipient of the data, storage time and the identity of the person in charge whom they can address is they wish to rectify, suppress or oppose el processing of the data.

For the **right to rectify**, incorrect or inexact data of those concerned will be corrected to serve the purpose of the process.

For **deletion rights** the data of those concerned will be deleted when the data holders express their non-conformity or opposition to consent of the processing of their data and there is no legal obligation that prevents them from doing this.

For the **right to portability** those concerned will have to communicate their decision and inform the person in charge, in this case, on the identity of the new person in charge to whom their personal data will be provided.

ANDSOFT will inform, all the persons that request the right to exercise their rights, on the terms in compliance with the rights of the person concerned, the manner and process in which they will come into effect.

7.1.3. SECURITY BREACHES OF PERSONAL DATA

When there is a security breach of personal data (ex: theft or unauthorised access to personal data, loss or removal of devices containing personal data, etc.) the competent authority shall be informed in a maximum delay of 72 hours from the moment in which the breach has been notified, unless the person in charge can prove, taking into account the principle of proactive responsibility, the unlikelihood that the breach in personal data security entails a risk to the rights and freedom of natural persons. If such a notification is not possible within 72 hours, a report on the reasons why the notification cannot be made must be sent.

Additionally, ANDSOFT must inform the person concerned, without delay, of the security breach of personal data in the case where it can entail a high risk to the rights and freedom of the person concerned, so that the necessary measures can be taken. The report must describe the nature of the personal data security breach and give the necessary recommendations so that the natural person concerned can deal with the potential adverse consequences resulting from this breach. The report must be sent to the person concerned as soon as reasonably possible and in close collaboration with the control authority, following his directives or those of other competent authorities, such as the law enforcement.

The designated person will write up a report in which it will be evaluated if the adequate technological protection was applied and if the necessary organisational measures were taken to immediately determine if there had been a safety breach of personal data and inform without delay the competent control authority and the person concerned. The report must inform whether the notice was given without delay considering, in particular, the nature and severity in the breach of security of personal data and the consequences and adverse effect for the person concerned.

7.2. TECHNICAL MEASURES

7.2.1. IDENTIFICATION

- Each AndSoft worker has a user profile created exclusively for each worker. This profile is used to access the computer and shared resources (Ex: SharePoint). Personal and private uses of the computer must be kept separate.
- Different levels of profile have been created (with admin rights to install or configure the user's system, without privileges or admin rights for access to personal data, amongst others), in order to prevent the access of non-authorised persons to personal data, or in the case of a cyber-attack to obtain special access or modify the operational system.
- To access the personal data stored in the system passwords are needed, that only those authorised users will have. The password will have 8 characters, a mix of numbers and letters.

- When various persons have access to personal data, each of these persons will need a user and password to have access.
- It is the obligation of all workers to guarantee the confidentiality of their passwords, avoiding their access to third parties.

7.2.2. OBLIGATION OF BACK-UPS

Below the technical measures employed to guarantee the back-up of personal data have been listed:

- **BACK-UP OF COMPUTERS AND DEVICES:** The devices and computers used to store, and process personal data will have to be kept updated.
- **MALWARE:** The devices and computers on which personal data is processed automatically must have an antivirus system installed to prevent the theft and the destruction of personal data. The antivirus will have to be periodically updated.
- **FIREWALL:** To avoid unwanted remote access to personal data an active firewall will be installed on all computer and devices on which personal data is stored or processed.
- **CODED DATA:** When personal data need to be taken outside the ANDSOFT offices, be it by physical means or electronical means (ex: remote control via laptops), the possibility of **encryption** must be considered to guarantee the confidentiality of personal data in the case of non-authorized access to this information.
- **BACK UP:** ANDSOFT does system security backups automatically every 24 hours, on a server that is not located at the workplace (hosting service company²).

Additionally, it is the responsibility of each worker to take the necessary security measures to avoid the loss of data: by doing regular backups on hard discs, by making back-up copies of work in progress on shared servers to which only authorised personal has access, by saving copies in servers in the cloud such as emails.

The security measures establish in the previous paragraphs will be revised periodically. Those revisions will be done either automatically (software or apps) or manually.

² Hosting company located in an EU country, with which we have signed a process control contract, additionally we have verified they meet the guaranties required by the RGPD.

7.2.3. GARANTIES OF OUR SUPPLIERS AND USER INFORMATION

At ANDSOFT we are aware that the protection of personal data does not end with ANDSOFT, because in some cases it is extended to our suppliers. That is why we commit to guarantying that they manage personal data in conformity with the RGPD.

In order to comply to this, ANDSOFT subscribes a specific contract of data processing management to each supplier that manages or can access any type of personal data as described in the GRDP.

Additionally, when giving consent to use the data, the user is informed that third party suppliers will have access to that personal data provided to the user and for what purpose.