General Policy for Personal Data Processing

S.I.F. Oltenia S.A.

Key Details
Policy prepared by: DECALEX DIGITAL S.R.L
Date of last revision: 10 June 2021

1. About Us

"We", S.I.F. Oltenia S.A., having its registered office in Str. Tufanele, nr. 1, 200767, Craiova, registered with the Trade Register under no. J16/1210/30.04.1993, sole registration code 4175676, hereinafter referred to as "**S.I.F. Oltenia S.A.**" are responsible for the processing of the personal data we collect from or about "you". For example, we will collect personal data from data subjects during participation in a personnel recruitment process, during a business relationship or when you use one of our services. Since we are based in the European Union, we process personal data pursuant to European data protection laws in force and also complying with national legal provisions.

S.I.F. Oltenia S.A. must gather and use certain information about individuals in its commercial relations. This data may include personal information about shareholders, suppliers, partners, collaborators, business contacts, employees and others, provided the organization has a relationship with them or may need to contact them.

This policy describes how this personal data must be collected, handled and stored in order to comply with the Company's data protection standards and comply with applicable law.

This Data Protection Policy ensures that **S.I.F. Oltenia S.A.:**

- Complies with data protection law and follows good practices
- Protects the rights of staff, shareholders and partners
- Is open about how they store and process data of individuals
- Protects itself from the risks of a personal data breach

2. Data Protection Laws

Regulation 679/2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data describes how organizations, including **S.I.F. Oltenia S.A.,** must collect, manage and store personal information.

These rules apply regardless of whether the data is stored electronically, on paper or on other media. In order to comply with the law, personal data must be collected and used fairly, stored securely and not disclosed unlawfully.

The Data Protection Law is based on the following important principles:

- personal data are collected and processed in a fair and transparent manner

- data collection and processing should be proportionate and necessary
- data collection and processing is done legally
- data collection and processing is done for specific, explicit and legitimate purposes
- the collected and processed data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- the collected and processed data must be accurate and up-to-date
- the storage of personal data is made for a limited period of time, in relation to the purpose for which it was collected and processed
- the processing is carried out in a way that ensures the adequate security of personal data
- the data is processed in accordance with the rights of the data subjects
- shall not be transferred outside the European Economic Area (EEA) unless that country or territory also ensures an adequate level of data protection

Policy enforcement

This policy applies to:

- The company **S.I.F. Oltenia S.A.** having its headquarters in the EU
- To all employees, volunteers and interns of **S.I.F. Oltenia S.A.**
- To all contractors, suppliers and other persons working on behalf of and for **S.I.F. Oltenia S.A.**

Data protection risks

This policy contributes to protecting **S.I.F. Oltenia S.A.** from certain data security risks, including:

- reputational damage,
- breaches of confidentiality,
- lack of access of the data subjects to their personal data.

3. What does Personal Data represent?

Personal data is information that directly or indirectly identifies persons as individuals. Indirectly means that they can be combined with other information, for example: name, postal address, email address and phone number, or a unique device identifier.

Responsibilities

Everyone who processes personal data for or with **S.I.F. Oltenia S.A.** has a certain responsibility to ensure that the data is collected, stored and handled properly. Each team that manages personal data must ensure that the data is handled and processed in accordance with this policy but also with the other data protection principles.

However, there are people in key positions regarding the responsibility of personal data:

1. **The administrator** is ultimately responsible for ensuring that **S.I.F. Oltenia S.A.** fulfils its legal obligations.

2. **The Data Protection Officer,** Decalex Digital Srl, is responsible for:
    - Maintaining management up-to-date on data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies in accordance with an agreed schedule.
    - Organising data protection training and counselling for persons covered by this policy.
    - Managing data protection questions from staff and from anyone else falling within the scope of this policy. Handles requests from individuals regarding personal data collected, held and processed by **S.I.F. Oltenia S.A.** (right of access to data).
    - Reviews and approves any contracts or agreements with third parties that could handle the company's Personal Data.
    - Maintains the connection with the National Supervisory Authority for Personal Data Processing (ANSPDCP).

3. The **IT Officer** is responsible for:
    - Ensuring that all systems, services and equipment used to store data comply with acceptable security standards.
    - Performing periodic checks and scans to ensure that the hardware and security software are working properly.
    - Assessing the acquisition of third party services that the Company intends to use for data storage or processing - e.g. cloud computing services.

General instructions on access to personal data

The only people who are able to access the data covered by this policy must be the ones who need it for their work.

Data should not be distributed informally. When access to confidential information is required, employees can request this from the department manager.

S.I.F. Oltenia S.A. will provide training to all employees to help them understand what their responsibilities are when handling data.

Employees must keep all data secure by taking precautions and following the guidelines below.

- In particular, strong passwords should be used and should never be shared. Personal data must not be disclosed to unauthorized persons, neither inside the company nor outside.
- The data should be reviewed and updated on a regular basis; if found to be old and no longer necessary for the purpose, it should be deleted.
- Employees should seek assistance from the Data Protection Officer if they are unsure about certain data protection issues.

4. The use of Personal Data

S.I.F. Oltenia S.A. will use personal data for the purposes described below. S.I.F. Oltenia S.A. does not collect or process more personal data or other types of data than those necessary for fulfiling our respective purposes. The Company will only use Personal Data as set forth in this General Personal Data Processing Policy, unless the person has expressly provided consent for another use of the data. If the Company wants to use the processed personal data for purposes other than those initially communicated, the Company will request the consent of the data subject. In cases where the processing is based on the consent of the data subject and the Company intends to use the data for a different purpose than the one for which the consent was obtained, this processing will only be possible with the permission of the data subjects.

Purposes of data collection and processing by S.I.F. Oltenia S.A. and the data involved

Purpose of processing	Data concerned by the processing
Conclusion, administration and performance of contracts	Name, surname, domicile, ID number and series, personal number (CNP), signature, Client ID, ID copy, payment information (account balance, bank transfer method), holding financial instruments.
Fulfilling legal obligations	Name, surname, domicile, ID number and series, personal number (CNP), Client ID, payment information (account balance, bank transfer method), bank card details, ID copy, client signature, contract termination request, holding financial instruments.
Prevention or identification of fraud	Name, surname, domicile, ID number and series, personal number (CNP), bank details (current account and issuing bank), payment information (account balance), holding financial instruments.
Defending our rights and interests or those of others	Name, surname, ID number and series, personal number (CNP), bank details (current account and issuing bank), payment information (account balance), holding financial instruments.
Improving services/ Promoting services offered by S.I.F.	Name and surname, telephone number, email address, mailing address, Client ID, number and date of concluding the contract.

Oltenia S.A.	
For performing service or collaboration contracts with third party suppliers or partners	In carrying out relations with suppliers and third parties, the Company may process personal data that allow the employee to be identified and contacted: name, surname, CNP, job.
For the internal employment process and for the performance of employment contracts	• Name, address, email address, telephone number and other contact information; • CV or cover letter, previous and / or relevant work experience or other experiences, education, transcripts or other information you provide to us in support of an application and / or application and recruitment process; • Information from interviews and telephone discussions you may have, if applicable; • Details on the type of job you are looking for, your current and / or desired salary and other terms relating to compensation and benefits packages, your desire for relocation or other job preferences and your preferred type of organisation. • Details on how you learned about the position you are applying for. • Any sensitive and / or demographic information obtained during the application or recruitment process, such as gender, information about your citizenship. • Health or medical information communicated by the candidate and / or data on racial or ethnic origin, religion. • Information from references and / or information received from background checks (if any), including information provided by third parties; and / or letters of recommendation. • Information relating to any history of previous employment relationships.

5. Data storage and security

These rules describe how and where data should be securely stored.

When data is stored on paper, it must be kept in a safe place where unauthorised persons cannot see it. These instructions also apply to data that is usually stored electronically but has been printed for some reason.

When not necessary, the document or files should be kept in a locked drawer or storage cabinet. Employees should ensure that documents and fingerprints are not left where unauthorized persons might see them, such as on a printer. Prints containing data should be securely disposed of when no longer necessary.

When data is stored electronically, it must be protected against unauthorized access, accidental deletion and attempted security breaches. Data must be protected by strong passwords that change regularly and never shared among employees.

If data is stored on removable media (such as a CD or DVD, USB stick), it must be kept well locked (stored in secure or encrypted spaces) when not in use. Data should only be stored on designated drives and servers and should only be uploaded to approved computerized cloud services. Servers containing personal data must be located in a secure location away from the general office space. Data should be backed up frequently. These backups should be tested on a regular basis in accordance with the standard backup procedures of S.I.F. Oltenia S.A. All servers and computers that contain data must be protected by approved security software and a firewall.

S.I.F. Oltenia S.A. takes data security seriously. We apply an appropriate level of security and therefore have implemented reasonable physical, electronic, and administrative procedures to protect the collected data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored, or otherwise processed.

Our information security policies and procedures are closely aligned with technological development and are periodically reviewed and updated as necessary to meet our business needs, technological changes and regulatory obligations.

Access to personal data is granted only to such personnel, service providers or affiliates/ collaborators of the Company, which justifies the need to know the respective information, motivated by the performance of the activity, or who request the information they need to perform their tasks.

In the event of a data breach containing personal data, the Company shall follow all the provisions of the laws in force regarding the notification of data breach.

Data Accuracy

The law requires the Company to take reasonable steps to ensure that the data is kept accurate and up-to-date. It is the responsibility of all employees who work with the data to take reasonable steps to ensure that they are kept as accurate as possible. The data will be organized in as few places as

necessary. The personnel shall not create unnecessary additional datasets. The personnel should take every opportunity to ensure that the data is kept up to date. For example, by confirming a candidate's details when the latter contacts the company.
S.I.F. Oltenia S.A. will facilitate the notification of the data subjects regarding the information that the Company has about them. For example, by means of a privacy notice displayed on the company's website. Personal data must be updated whenever inaccuracies are discovered. For example, if a data subject can no longer be contacted on the stored phone number, he/she must be removed from the database.

Lawfulness of processing personal data

S.I.F. Oltenia S.A. bases the processing of data on the following legal grounds:

- Consent for processing activities in the purpose of promoting company services;
- Legitimate interest in communicating with the shareholders of S.I.F. Oltenia S.A.;
- Performance of a contract to which the data subject is a party;
- Fulfiling a legal obligation. For example, to comply with a legal obligation under our responsibility regarding mandatory tax reporting, preventing and combating money laundering and terrorist financing, periodic auditing, etc.

The Romanian law requires us to keep personal data, for legal and compliance reasons, such as: the prevention, detection and investigation of a crime, the prevention of loss, fraud or any other abuse of our services and information systems. We may also use personal data for information security purposes, or to protect or enforce our privacy, security, or proprietary rights, or those of others.

Personal Data Storage Period

In general, the Company will delete the collected personal data if they are no longer necessary to achieve the purposes for which they were originally collected. However, due to legal provisions, the company is obliged to store personal data for a longer period.

Thus, the Company:

- **Recruitment Data:** Will store recruitment data for a minimum of 12 months and a maximum of 18 months, and after this deadline, the company will start the procedure for obtaining the candidate’s consent to further store this information in the database. In order to protect the interests of the Company, the minimum period imposed by the Romanian legislation for the storage of the Recruitment Data is 12 calendar months, a period imposed by art. 20 of the G.E.O. 137/2000 on the prevention and sanctioning of all forms of discrimination. Taking into account the specificity of the company's activity, the processing of personal data is "necessary" for carrying out the main activity of the company, that of personnel recruitment. Moreover, the collection and processing of data by the data subject is indispensable for the recruitment of personnel, so that it is justified to store data for a maximum period of 36 months.

- **Employee data:** Will store the data of its own employees for the period necessary for the performance of the individual employment contract in accordance with Law 53/2000.
- **Marketing:** Will store the data of natural persons processed for advertising purposes, for a period of 12 months, and after reaching the deadline it will take the necessary steps to renew the legal basis of the processing.
- **Shareholders' data**: They will be kept for as long as the latters are shareholders. In case of losing the shareholder status, for example following the sale of the shares, the shareholders' data will be archived for a period of 10 years, according to the applicable legal provisions in fiscal, accounting matters.
- **Personnel file:** After the termination of the employment contract, the Company, in accordance with OMEF 3512/2008, MFP Order no. 2634/2015 and Annex 6 of the Law on National Archives, is obliged to comply with the following deadlines for the storage of human resources documents:
  - Salary payrolls – 50 years after their creation
  - Personnel files, employment contracts, civil service conventions – 75 years after their creation

6. Consent

The Company shall obtain consent through a written statement, including in electronic form, or verbally. The consent shall cover all processing activities carried out for the same purpose or purposes. If the data processing is made for more than one purpose, the consent will be obtained by the Company for all processing purposes.
Regardless of the purpose for which consent is obtained, the consent statement does not contain information on other matters.

All consent statements used by the Company shall comply with the following conditions:

- will state the purpose for which consent is sought
- the statement is intelligible and easily accessible, using clear and simple language
- the data subject’s right of withdrawal, at any time, in a way as simple as it has been obtained

Special data categories
It is possible, in certain cases, for the Company to process special categories of personal data (“sensitive data”). Sensitive data refers to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric data, with the aim of uniquely identifying a natural person, a natural person's health or sex life or sexual orientation. For example, we may process sensitive data that a data subject/employee has explicitly made public. The Company may also process sensitive data as necessary for the establishment, exercise or defence of a legal right.

The Company will also process sensitive data when the data subject has freely consented in advance, expressly and separately in a specific context, for a specific purpose, such as psychological testing.

Under the national legislation in force for the company's own employees, **S.I.F. Oltenia S.A.** may collect the data of minors who have the quality of children or any co-insured persons of the employees. This data is necessary to obtain the status of insured person at the National Health Insurance House and to benefit from the free medical services in the state medical system. We mention that this processing is a legal obligation and therefore does not require the parental consent for the processing of the data of the concerned child.

The company **S.I.F. Oltenia S.A.** collects and processes special data on the health of its employees. The legal basis for the collection and processing of this type of data is Law 53/2000 and Law 319/2006.

7. Sharing personal data

The Company will disclose personal data only for the purposes and to those third parties that are described below. **S.I.F. Oltenia S.A.** will take the necessary measures to ensure that your personal data are processed, secured, and transferred in accordance with the law in force.

1. **S.I.F. Oltenia S.A.**

The personal data of candidates, employees, shareholders, partners or service providers may be transferred to one or more Group companies. Except for this situation, the company does not disclose the personal data of the participants in the recruitment process to third parties outside the company

2. **External Service Providers**

Where necessary, the Company will employ other companies and individuals to perform certain tasks that contribute to our services, on our behalf, within the framework of data processing agreements. For example, we may provide personal data to agents, contractors or partners for hosting our databases and applications, for data processing services, for communicating with the data subject, or for providing support or interview services within personnel training projects. The Company shall share and make available to external service providers only such data and to the extent necessary for that purpose. Such data may not be used by them for any other purpose, for their own purposes or for the purposes of third parties. External Service Providers of **S.I.F. Oltenia S.A.** are bound by contract to respect the confidentiality of personal data.

3. **Public authorities**

When a public authority or any other state institution or body requests personal data from the Company, under a legal obligation, we are obliged to make it available to them.

8. Data subject's rights

Data subjects have specific legal rights with regard to the personal data that the Company collects. **S.I.F. Oltenia S.A.** will respect these rights and assures you that it takes due account of the data subjects' interests.

Information on the legal rights arising from the data protection legislation in force:

- **The right to withdraw their consent:** if the processing of personal data is based on the consent of the data subject, they may withdraw their consent at any time, following the procedures described in that consent form. The company ensures that the agreement can be withdrawn by the same means as it was given, for example, electronically.

- **The right to rectification:** The Data Subject may obtain from the Company rectification of the personal data concerning him/her. The Company will make reasonable efforts to ensure that the personal data in its possession or under its control is accurate, complete, current and relevant, based on the most recent information available to the Company.

- **The right to restriction:** the data subject may obtain from the Company restrictions on the processing of his/her personal data, if:
    - he/she challenges the accuracy of personal data for the period in which we need to verify accuracy,
    - the processing is unlawful and he/she requires the restriction of the processing rather than the erasing of personal data,
    - the company no longer needs the personal data, but the data subject requests them for the establishment, exercise or defence of a right, or
    - the candidate objects to processing during the period which the Company verifies whether our legitimate grounds take precedence over the data subject's.

- **The right to access:** The Data Subject may request information about the Personal Data the Company holds, including information about what categories of Personal Data the Company has in its possession or control or for what purpose, where they are used, where they are collected from if they do not come directly from the Data Subject, and to whom they have been disclosed, if any. The Data Subject may obtain a copy from the Company, free of charge, with the personal data it holds about him/her. The Company reserves the right to charge a reasonable fee for each additional copy that the data subject may request.

- **The right to portability:** At the data subject's request, the Company will transfer the personal data to another controller, where technically possible, provided that the processing is based on the data subject's consent or is necessary for the performance of a contract. Instead of receiving a copy of the personal data, the Data Subject may request the Company to transfer the data directly to another controller.

- **The right to erasure:** The Data Subject may obtain from the Company the right to have his/her personal data erased, when
    - personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
    - he/she has the right to object to the further processing of personal data (see below) and to enforce this right to oppose the processing;
    - the processing is based on the consent of the person – if the data subject withdraws his/her consent, there is no other legal basis for the processing of the data;

Unless processing is required:

- in order to fulfil a legal obligation that requires our processing;
- in particular for the statutory data retention requirements;
- for the establishment, exercise or defence of a right.

- **The right to object:** The data subject may object, at any time, to the processing of personal data, due to his/her particular situation, if the processing is not based on consent, but on our legitimate interests or those of a third party. In this case, the Company will no longer process his/her personal data unless we can demonstrate with valid and legitimate reasons and a major interest in the processing or in the establishment, exercise or defence of a legal right. If the person objects to the processing, he/she will have to specify whether he/she wants to erase the personal data or restrict its processing.

- **The right to submit a complaint:** We recommend that, for any doubt or dissatisfaction about how S.I.F. Oltenia S.A. manages your personal information, you contact our Data Protection Officer. In case the information provided by our Data Protection Officer is not satisfactory or you are dissatisfied with the way in which S.I.F. Oltenia S.A. has dealt with a complaint or request regarding this data, you are entitled to submit a complaint to a data protection supervisory authority:

    - The National Supervisory Authority for the Processing of Personal Data by filling in the online form available at: dataprotection.ro/?page=Plangeri_pagina_principala

Rules on requests for access to personal data

- **Time period:** S.I.F. Oltenia S.A. will try to fulfil the request within 30 days. However, the period may be extended for specific reasons relating to the specific legal right or complexity of the request.

- **Access restriction:** In certain situations, S.I.F. Oltenia S.A. may not allow access to all or part of the personal data of the person who made the request, due to legal provisions. If the Company refuses the request for access, the data subject will be informed of the reason for the refusal.

- **Impossibility to identify:** In some cases, it is possible that S.I.F. Oltenia S.A. may not be able to search for the requested personal data, due to the identification data that the data subject provides in the application. In such cases, when the Company is unable to identify him/her as the data subject [subject of the data], it is unable to respond to the request to enforce the legal rights as described in this section, unless the person provides additional information allowing its identification.

- **Exercise of legal rights:** For any other information on how to process personal data (including to exercise your rights above), the data subject may contact our Data Protection Officer, in writing, by e-mail to dpo@sifolt.ro, or by sending a letter to the registered office in Craiova, str. Tufănele nr. 1, jud. Dolj, Romania.

9. Storing and transferring work data

The employees of **S.I.F. Oltenia S.A.** receive a variety of resources to do their job efficiently and quickly. But it is important that these resources be carefully preserved.

The storage, transfer and sharing of information may result in personal data breaches.

1. **E-mail**

All personal data sent by email (as an attachment or in an email text) should be considered sensitive and protected as such. The employees never send personal data documents to a person outside the company unless they have notified the Data Protection Officer. This action includes sending company emails to the employee's own personal email account.
Not all employees of **S.I.F. Oltenia S.A.** have access to the same information. Before sending data or files to another employee in an email, contact your manager to make sure that the recipient is allowed to have access to it.

2. **Account and cloud storage apps**

We know that sometimes employees may need access to work outside the office, at home, from mobile devices or other company equipment. However, job information should not be stored or shared in personal accounts or cloud applications such as iCloud, Google Drive, Box, Dropbox, Microsoft OneDrive, etc. Outdoor access to company servers will be made via secure connections and only with the approval of the IT department.
In case you need to store or perform online backups, it must be approved by the IT department.

3. **Physical storage devices**

The storage of work data on physical devices, including, but not limited to, USB drives, memory cards, CDs, or external hard drives, must be pre-approved by the company management.
Company employees must only use devices supplied by the Company, unless otherwise permitted.
For technical security reasons, the company **S.I.F. Oltenia S.A.** has prohibited the use of USB ports.
NEVER use or even connect a USB drive that you have found or been given as a promotional item. These devices may contain hidden malware or viruses.
Lost or stolen devices must be reported to IT and an immediate manager to ensure their safe return and prevent data leakage.

Business Transfers

In connection with any reorganization, restructuring, merger or sale or other transfer of assets (collectively, the "Business Transfer"), we will transfer data, including personal data, in a reasonable amount and as required for the Business Transfer, and provided that the Receiving Party agrees to deal with your Personal Data in a manner that complies with applicable data protection laws. The Company will continue to ensure the confidentiality of any personal data and notify affected users before personal data becomes subject to another privacy policy.

Public bodies

We will disclose personal data of data subjects only to public bodies, where this is required by law. **S.I.F. Oltenia S.A.** will respond, for example, to requests from courts, law enforcement agencies, regulatory agencies and other public and governmental authorities, which may include authorities located outside your country of residence.

10. International transfers of personal data

Under special circumstances, it will also be necessary for **S.I.F. Oltenia S.A.** to transfer personal data to countries outside the European Union/European Union Economic Area (EEA), to so-called "countries outside the European Union". Such transfers to third countries may relate to all processing activities described in this General Personal Data Processing Policy.

This Policy applies even if we transfer personal data to third countries, where a different level of data protection applies than in the country of residence. In particular, an international data transfer may take place in the following situations:

Other non-EU / EEA third parties

All transfers of personal data to third parties outside the Company shall be made with the prior notice and, where applicable, with the consent of the data subject. Any transfers of personal data to countries other than those for which a decision has been taken on the adequacy of the level of data protection by the European Commission, as listed on the official websites, shall be made on the basis of contractual agreements using the standard contractual clauses adopted by the European Commission or other appropriate safeguards, in accordance with the law in force.

11. Amendments to this Policy

The Company reserves the right to amend this General Personal Data Processing Policy and will make changes to this Policy at any time. The Company will also keep previous versions of this Policy in an archive, for reference.