SOGRAPE

ORIGINAL LEGACY WINES

SOGRAPE

PRIVACY POLICY

General Data

Protection Regulation

Introduction

The General Data Protection Regulation (GDPR) regarding to the processing of personal data and on the free movement of such data has came into force on the 25th May 2016 and has repelled Directive 95/46/EC.

The main purpose of the Regulation is to restore the control of personal data to European citizens, avoiding the spread and misuse and/or abuse of their personal data.

As a Regulation, it is directly applicable in all Member States, ensuring a consistent and high-level legislation on Data Protection.

This Regulation has provided a transitional period of 2 years for organizations to adapt to this new reality, becoming applicable on the 25th May 2018. This new legal framework changes the paradigm on how organizations process personal data, whose impact varies according to the size of the organization, the business sector, the nature of the collected data and the method of personal data processing.

The rights of a data subject object of a processing are reinforced by the need of consent in processing of personal data where there is no other lawfulness basis, the right to easy access and rectification of data, the right to information, to be "forgotten", the right to object the processing of personal data and the right to data portability.

It also provides general obligations for controllers and processors, including the obligation to implement technical and organizational measures, taking into account the risk in the processing of personal data. These measures should be appropriate and necessary to ensure compliance with the Regulation.

The provisions of this Policy are applicable to the relationships Sogrape Group maintains with its Customers, Suppliers, Partners and other professionals related with its commercial activity.

This Policy applies to transactions carried out in Portugal or with Portuguese personal data.

Definitions

1. **Personal data:** Information relating to an identified or identifiable natural person («data subject»); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
2. **Special categories of personal data:** Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data (means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question), biometric data (means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data) for the purpose of uniquely identifying a natural person, data concerning health (data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status) or data concerning a natural person's sex life or sexual orientation.
3. **Data concerning health:** Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
4. **Controller:** A natural or legal person, which determines the purposes and means of the processing of personal data.
5. **Processor:** A natural or legal person, which processes personal data on behalf of the controller.

6. **Data subject:** A natural person owner of the data processing to "whom the information is related".
7. **Processing personal data**: Any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
8. **Data protection officer**: A person designated by the organization that will be involved in all matters relating to the protection of personal data and responsible to monitor compliance with this Regulation**.**

Principles relating to processing of personal data

Sogrape Group processes personal data of customers, suppliers and employees with respect to the following principles:

- **Principle of information adequate, relevant and necessary ("Data Minimisation") (Article 5 (1) (c) of GDPR)**

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. These are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The personal data collected should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This is one of the new concepts introduced that should guide the entire process of processing personal data, Privacy by Default, which means mechanisms should be introduced to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are collected.

Sogrape Group processes personal data many times during its activity. In this regard, the data requested from customers, suppliers and even employees are restricted to the necessary purposes for which they are collected.

- **Principle of purpose limitation**

The personal data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This principle that is established in article 5 (1) (b) of GDPR, implies that when Sogrape Group companies collect data for one or more purposes, this processing shall be compatible with the purposes for which they were originally collected.

- **Principle of accuracy**

The companies that integrate the Sogrape Group guarantee the updating and possibility of rectification of the personal data in order to guarantee the accuracy of the data in its databases.

In order to comply with this principle, it was adopted reasonable measures to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- **Principle of storage limitation**

Personal data subject to a processing, as stated by the principle of purpose limitation, are collected to for specified, explicit and legitimate purposes (article 5 (1) (e) of GDPR).

Once the time required for the purposes for which they are processed is over, the data is either eliminated or anonymised.

- **Principle of integrity and confidentiality**

Personal data shall be processed in a way that guarantees confidentiality and security in order to not cause damage to the data subject judicial sphere (Article 5 (1) (f)).

- **Principle of accountability**

Sogrape Group companies, pursuant to article 5 (2) of the Regulation, are responsible for complying with all principles listed above and must be able to evidence it.

Rights of the data subject

Sogrape Group companies guarantee customers, suppliers and employees rights regarding data protection and the necessary measures to provide information and any communication regarding the processing of personal data in a concise, transparent, intelligible and accessible, using clear and simple language.

This information shall be submitted in writing or by electronic means or, if requested, information shall be provided orally.

It is important that each company of Sogrape Group take measures to ensure that the natural personal requesting the personal data is the data subject. If the company has reasonable doubts to identify the natural personal performing the request, each company may request additional information to confirm the identity of the data subject.

If the company does not take action on the request of the data subject within one month of receipt of the request, it shall inform the data subject of the reasons for not taking action and on the possibility of lodging a complaint within a supervisory authority as well as seeking a judicial remedy.

The information and notifications of measures should be granted free of charge. However, if the applications are unfounded or excessive, the company may either: i) or require payment of a reasonable fee in respect of its costs; ii) or refuse to comply with the request.

The data subject may also request that their data be completely erased from the companies data bases without undue delay.

Sogrape Group companies may only grant this right in the following situations:

a. The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b. The data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
c. The data subject shall have the right to object, on grounds relating to his or her particular situation, pending the verification whether the legitimate grounds of the controller override those of the data subject;
d. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing;
e. The personal data have to be erased for compliance with a legal obligation;
f. The personal data have been collected in relation to the offer of information society services;
g. When the retention period defined for the data has been exceeded.

However, Sogrape Group companies shall not apply to the extent that processing is necessary:

a. For exercising the right of freedom of expression and information;

b. For compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a

task carried out in the public interest or in the exercise of official authority vested in the Controller;

c. For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e. For the establishment, exercise or defence of legal claims.

The data subject shall have the right, without undue delay, to correct inaccurate data.

Processors

As part of the processing personal data, Sogrape Group companies rely or may rely on third parties, mandated by it, for, on behalf of each entity of Sogrape Group, and in accordance with the instructions provided, to proceed with the processing of personal data in strict compliance with the provisions of the law and with this Privacy Policy.

These processors may not transmit personal data to other entities without each Sogrape Group company has given its prior written authorization to do so, and are also prohibited from hiring other entities without Sogrape Group company's prior authorization.

Sogrape Group companies are committed to subcontract only entities that offer the maximum security in the implementation of the appropriate technical and organizational measures, in order to guarantee the defense of the data subject's rights.

All entities subcontracted by the companies of Sogrape Group shall be bound by the means of a written agreement, which covers the object and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects and the rights and obligations of the parties.

Security of personal data

The Sogrape Group companies have implemented appropriate technical and organizational measures to ensure a level of security appropriate to the risk in order to prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

It is necessary to take into account the potential vulnerabilities of the system and predict the impact that these vulnerabilities can cause and affect people in order to assess risks and define the measures that best suit them. After the impact assessment has been carried out, the result of this evaluation may influence the measures to be adopted.

Sogrape Group companies may freely select the means they consider appropriate and the GDPR only establishes an obligation of result to the controller.

The measures to be adopted will dpeend on what is considered necessary for each specific case, such as:

i) the pseudonymisation and encryption of personal data;
ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Personal Data Breach

Personal data breach means a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Detection of an information security incident may occur due to a number of different situations (e.g. an employee loses the laptop and reports the incident, a customer checks an anomalous situation and communicates it to a collaborator, a security team detects suspicious activity behavior of an application).

The data breach may occur from:

a. **Confidentiality Breach**: whenever disclosure of or access to personal data is made in an unauthorized or accidental use;
b. **Availability Breach**: whenever there is loss of access or destruction of personal data in an unauthorized or accidental use; and
c. **Integrity Breach**: whenever personal data is altered in an unauthorized or accidental manner.

In case of data breach, the controller shall notify the Superiority Authority without undue delay and, where possible, within 72 hours of becoming aware of it, unless it there is no risk to the rights and freedoms of natural persons.

If the notification to the Supervisory Authority is not performed within 72 hours, it shall be accompanied by the reasons for the delay.

In the case the company is a processor the notification is made to the controller, without undue delay.

Apart from the notification to the supervisory authority, it may also be necessary to report the data breach to the data subject. This communication is necessary when the data breach is

likely to imply a high risk for rights and freedoms of natural persons. In such cases, the controller shall report the data breach to the data subject, without undue delay.

Information to describe the extent of the security incident includes, for example, estimation of the number of data subjects affected by the data breach, moment and duration of incident and permanent or temporary consequences.

Sogrape Group companies, as controllers, shall document any personal data breaches. This documentation shall include the facts relating to the breaches, the effects and the extent to which it has been adopted in order to enable the supervisory authority to verify compliance with these requirements.

On the other hand, Sogrape Group companies shall ensure a corrective action plan in order to avoid future replication.

Sogrape Group companies are responsible for keeping a record of evidence of the corrective actions being implemented (eg. a test report that confirms that the vulnerability that gave rise to the breach of personal data has been corrected).

Examples of technical and organizational resolution measures include, among others:

a. The change of passwords in operating systems and/or applications impacted by the data breach;

b. The revocation and generation of new digital certificates for impacted services and / or applications;

c. Revoking user account sessions on impacted systems and / or applications;

d. The communication to users of duty to change credentials in impacted systems and/or applications;

e. The formatting and reinstallation of systems and applications in impacted equipment;

f. The recovery of information through existing backups to the last state considered valid.

Exercise of rights

The right of access, rectification, erasure, restriction of processing, data portability and to object, can be exercised by the data subject by contacting the respective Sogrape Group company through the e-mail privacy@sogrape.pt.

The respective Sogrape Group Company will reply in writing (including by electronic means) to the data subject's request within a maximum period of one month from the receipt of the request, except in particularly complex cases, for which this period may be extended up to two months.

Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the Sogrape Group company may charge a reasonable fee based on administrative costs, or refuse to act on the request.