Data Protection Policy
of
Sphera Franchise Group SA
and its Subsidiaries

This Policy covers Company and Staff procedures, required for complying with the applicable data protection laws, including GDPR, in terms of the daily activity

Contents

Related Policies
This Policy shall be supplemented by the following additional documents:

- The Security Policy on Personal Data Processing
- The Data Retention Policy
- The Information Classification Procedure

Purpose
Describing the processes and procedures which the Company has implemented in order to comply with the European data protection legislation. References herein to the "Company", "we", "us" shall mean **Sphera Franchise Group SA**, together with its subsidiaries, namely the following companies: **US Food Network SA**, **American Restaurant System SA**, **California Fresh Flavors SRL**, unless otherwise specified.

This Policy is based on the following principles: **Lawfulness, Equity and Transparency, Purpose Limitation, Data Minimization, Data Accuracy, Data Retention, Security, International Transfers, Rights of Individuals and Responsibility.**

Scope
This document covers all categories of Personal Data processed by the Company, either electronically or in structured paper files, in particular in its capacity as Data Controller.

It applies to all Company legal representatives, managers, *both executive and non-executive ones*, directors, officers, and employees (who, for the purposes hereof, also include temporary employees, hired staff and contractors) (collectively referred to as "**Staff**" or "**the Staff**"). The Staff shall read, understand and adhere to this Policy and the applicable law.

All Company managers, officers and directors are required to implement this Policy and to ensure that the employees, individuals and entities for whom they are liable have been informed of, understand and adhere to the requirements hereof. Any violation of this Policy shall be reported to the Data Protection Officer.

Willful or negligent non-compliance by the Staff of the European data protection legislation or this Policy shall constitute a disciplinary offense that may, in some cases, be considered a serious offense, which shall be handled in accordance with the disciplinary procedures of the Company.

Failure to comply with this Policy may also imply that the Staff are directly responsible for the penalties laid down by the European data protection legislation. In particular, unauthorized use by an individual of personal data obtained as a result of being employed by the Company constitutes a criminal offense.

This Policy does not replace national laws, regulations and codes of conduct applicable to data protection and confidentiality, and, instead, has been developed in line with the interpretation of the provisions of the General Data Protection Regulation ("GDPR"). Local laws shall be observed at all times and shall take precedence over this Policy if

they provide for stricter data confidentiality and data protection standards. Any variation shall be set forth in an Annex to this Policy. Additional guidance for specific teams may occasionally be issued.

Please consult the Data Protection Officer or the Legal Department team if you require any advice, help or assistance on any topic covered by this Policy.

The Company has chosen to officially designate a Data Protection Officer ("DPO").

The Data Protection Officer ("DPO")

Contact details:

- protectiadatelor@spheragroup.com
- protectiadatelor@kfc.ro
- protectiadatelor@pizzahut.ro
- protectiadatelor@pizzahutdelivery.ro
- protectiadatelor@taco-bell.ro

Key Definitions

The **data controller** is a person or body that (alone or jointly with others) determines the purposes and means of processing personal data. For the purposes hereof, the Company is deemed to be a Data Controller.

The **data processor** is any legal or natural person that processes data on behalf of the Data Controller, for example, the Company's outside IT provider.

Personal data mean any information relating to an identified or identifiable natural person, such as our customers, business partners, employees, or any other persons. Personal data include the name, address, date of birth or personal financial and banking information. An identifiable person is one who can be identified, directly or indirectly, by reference to an identifier, such as the name, the identification number, or one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. Personal data include pseudonymized data, but not information that is truly anonymous and may include opinions and facts about people, as well as CCTV video or audio recordings. **The fact that the information is publicly available (for example, on LinkedIn) does not prevent the application of data protection laws.**

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

Pseudonymized data mean Personal Data that have been processed so that they could no longer be traced back to a particular person without the use of additional information.

Processing is widely defined to cover any operation or set of operations which is performed upon personal data, including collection, storage, use, disclosure and

destruction thereof. Most certainly, the Staff shall process certain personal information about customers who are individuals, as well as other Staff and business contacts.

Special categories of data are Personal Data that benefit from special legal protection in accordance with the applicable law. They include **racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purposes of uniquely identifying a person, health, sex life or sexual orientation**. The processing of data on criminal offenses and administrative infringements ("**data on criminal offenses**") is also prohibited or restricted by the applicable laws. For example, medical and other health-related information about the Staff shall be a special category of data.

Statement on the Data Protection Policy

The confidentiality of the staff, suppliers, business partners, customers and other individuals in respect of whom Personal Data are processed during the provision of investment management services is extremely important to the Company. The protection of their Personal Data and their use in as fair and trustworthy a manner as possible is crucial to the Company's core values and is an important element in maintaining its relationship and reputation with its customers.

European Principles on Personal Data Protection

The Company is fully committed to complying with its obligations under the European data protection legislation, whenever it processes personal data. To this end, the Company fully accepts the data protection principles outlined below.

Principle 1: Lawfulness

We may only process Personal Data for which we have a legal basis, as set out in the data protection legislation:

- For the purposes of our legitimate business interests (or those of a third party), provided that such interests do not harm the interests or rights of the data subjects (for example, to ensure the effective management of our Staff or to ensure that our Staff provide good services to our customers); or
- For fulfilling a legal obligation (e.g., for tax purposes or to report an incident to the law enforcement authorities).

The processing of personal data may also be carried out with the consent of the relevant data subject, in compliance with the requirements for obtaining valid consent, in accordance with the data protection legislation. Consent may be necessary, for instance, for the purposes of marketing and using cookies and similar technologies on the Company websites.

Additional (and more restrictive) reasons apply to the processing of special categories of personal data and data on criminal offenses. They are very limited under the European data protection legislation and, in the context of investment data, only four reasons show potential relevance. These include processing that is (i) substantially in the public interest, under the Union or Member State law; (ii) data that have been

clearly made public by the data subject; or (iii) data that are processed with the explicit consent of the data subject.

- The Staff shall ensure that there is a legal basis for any Personal Data processing for which they are responsible. The Staff shall request guidance from the Data Protection Officer if they wish to process Personal Data on the basis of consent.
- If Staff need to request additional Personal Data or if they change the manner in which Personal Data are processed, they will always consider whether the Personal Data or the changes concerned have a legal basis.

Principle 2: Equity and Transparency

In order to be fair and transparent, we shall inform individuals about how their Personal Data are processed in a concise, transparent, comprehensible and easily accessible way, using clear and simple language. Said information should include: which personal data we process, how we intend to use such data, with whom we share them, whether we intend to transfer the data to another country outside of the European Economic Area, and how people can reach us in view of asking questions or exercising their rights.

We do this for our employees via "Employee Information" and for our website visitors, in the Policy on Confidentiality and Cookies, as well as the Personal Data Processing Policy, available on the Company website.

- If Staff must request further Personal Data or change the manner in which Personal Data are processed, they will always keep in mind that additional information must be submitted to the relevant individuals. The Staff shall pay particular attention to providing information about any use of Personal Data which the data subject would not expect.

Principle 3: Restrictions

Personal Data shall only be used for the purposes for which they have been collected. The Staff shall not use Personal Data for any purpose other than that in respect of which they have notified the individual or which would not be obvious to that person (or compatible with the original purpose), e.g.:

- The Staff shall only disclose Personal Data to persons who, by virtue of their position or commercial activity, must learn such information in order to carry out their duties in accordance with the stated purposes;
- To determine whether a new purpose of the processing is compatible with the original purpose, the Staff shall consider any link between the purposes, the context in which the Personal Data have been collected and the relationship between the parties, the nature of the Personal Data, the possible consequences of any future processing and any proposed guarantees; and
- The use of Personal Data for new purposes may, in certain limited circumstances, require the transmission of information or the obtaining of authorizations from the competent data protection authorities. It may also require consultation with workers' representatives. The Staff shall consult with the Data Security Officer when having any questions as to whether a particular use of Personal Data is permitted or not or if they wish to use Personal Data for a new purpose.

Principle 4: Data Minimization

The Personal Data which we collect shall be adequate, relevant, and limited to what is necessary for the purposes for which they are collected. We shall not ask for more Personal Data than we actually need in view of the legal basis for which we collect them. We shall check the relevance of the Personal Data collected by our Staff on a regular basis to ensure that they are still proportionate to the purpose.

The following minimization techniques should be considered whenever practicable:

- **Less is more:** Always Ask yourself "Do we need to collect this information in order to reach our goals?" An example of over-collecting Personal Data would include sending a general questionnaire to job applicants including specific questions about family members and relatives, which is a collection of information that will not be used.
- **Anonymization:** If a data set that includes Personal Data can be anonymized, then it should be. This reduces the risk of injury to the persons involved and removes such data from the scope of this Policy (please note that data may only be considered truly anonymous if it is not possible to re-identify a person based on such data or other data in our possession).
- **Pseudonymization:** If anonymization is not possible, consider whether personal data may be the subject of pseudonymization, which is the technique of processing personal information so that it should no longer be traced back to a particular person without the use of additional information to be kept separately and subject to technical and organizational measures that ensure non-application.

Principle 5: Data Accuracy

Personal Data shall be accurate and up to date. We will encourage individuals to let us know about any changes in their personal data (and to update, rectify or delete the records accordingly).

- The Staff should not use Personal Data which they suspect might not be up to date without confirming their accuracy.
- The Staff shall ensure that personal information is accurately captured and is managed in accordance with the business rules applicable to each system. Any irrelevant or obsolete information should be safely removed and deleted, in accordance with our Data Retention Policy.
- Recurrent opportunities shall be given to the Staff to verify the Personal Data relating to them which we hold and they shall promptly inform their respective line managers about any changes in their Personal Data or any circumstances that may affect the records kept about them (e.g. address, banking information). Any changes shall be made promptly.
- If the Staff learn about a change in the data of a customer or other person, the relevant databases shall be updated without delay.

Principle 6: Data Retention

Personal Data shall not be retained for longer than necessary to meet the legal purpose for which they have been collected. Then, they shall be safely deleted. This requirement is subject to other laws and obligations that require us to keep information for certain periods of time.

If Personal Data cannot be deleted (or anonymized) because, for instance, the archived tapes are kept in a third-party storage location, the principle listed above will be fulfilled if such information is "obsolete", provided that:

- We are unable or we do not attempt to use said Personal Data to inform about any decision concerning any person or in a manner that affects that person in any way;
- We do not grant any other organization access to said Personal Data;
- We surround said Personal Data with the appropriate security methods from a technical and organizational standpoint; and
- We undertake to delete the information permanently and safely if or when possible.

Principle 7: Security

Personal Data shall be kept and used safely and shall be protected against unauthorized or unlawful processing and against loss, accidental destruction or damage. This applies to our computer systems, websites, and daily handling of Personal Data. We shall at least comply with any security and organizational measures required by law.

The Designation of the Data Processors

If the Company (as the Data Controller) employs another organization to process Personal Data on its behalf, said organization (the "Data Processor") shall have implemented "appropriate technical and organizational measures" to meet the requirements of the European data protection law and to ensure the protection of the rights of individuals. Within this process, a written contract with the Data Controller shall be concluded, containing specific contractual obligations.

If the Company acts as a Data Processor on behalf of the Franchisor (*i.e. YUM! Restaurants International*) (the Data Controller), **it may not hire another data processor without the prior written specific or general consent of the Data Controller**. In the case of a general written consent, the Company shall inform the Data Controller of any intended changes in terms of adding or replacing other data processors, thus giving the Data Controller the opportunity to oppose such changes. It shall ensure that it reduces the flow of relevant obligations to the sub-processors.

- Any Staff member responsible for designating a Data Controller shall ensure that all contracts contain appropriate provisions and that they have conducted a check of the Data Controller's security measures to ensure that they comply with Company requirements.
- The Company shall perform regular inspections and audits of the systems, records, premises, staff and any other materials used to provide the relevant services in order to verify whether the Data Controller (and any sub-processors) meets its contractual obligations and any other obligations under the applicable European data protection laws. An audit-related provision shall be included in the written contracts.

Principle 8: International Transfers

European data protection rules restrict transfers of Personal Data outside the EEA (including to other Group companies and external Data Controllers), unless there is adequate protection of the Personal Data or measures have been taken to ensure Personal Data protection. The Company may occasionally export to other parties outside the EEA. If so, we shall proceed in accordance with the standard contractual clauses approved by the European Commission regulating transfers of certain Personal Data between us and other members of our Group.

There is a (limited) number of other situations in which Personal Data may be transferred outside the EEA, including:

- When they are sent to a country or territory, or an international organization recognized by the Commission as providing appropriate protection (also possibly including US organizations that are certified by the EU-US Privacy Shield);
- Reliance on mandatory corporate rules;
- When the individual has explicitly agreed to the transfer;
- When they are required to implement a contract;
- When they are required for reasons of substantial public interest; or
- When they are required for the establishment, exercise or defense of legal claims.

Please ask for advice from the Data Protection Officer if:

- A third party is to process Company Personal Data outside the EEA (not only if said third party is established outside the EEA, but also if the Personal Data is to be held or accessed remotely by a third party or by its subcontractors at a location outside the EEA); or
- There are any questions as to which Personal Data may be transferred outside the EEA.

Principle 9: The Rights of Individuals

We shall always respect the rights of individuals under the European personal data protection legislation (to the extent applicable), namely:

- To receive information about how their Personal Data is being processed (please see the Equity and Transparency section above for further details);
- To access and rectify the related Personal Data;
- To delete or restrict the processing activity;
- To transfer Personal Data to another Data Controller;
- To oppose certain processing methods in special situations; and
- Not to be subject to the use of fully automated decisions (including profiling) that cause legal effects or significantly affect individuals.

We shall respond to any requests without undue delay and, generally, within one month of the receipt of the relevant request.

- The Staff requests to view their records or to exercise any of their other rights under data protection laws should be submitted in writing to the Data Protection Officer, who shall take the appropriate steps to respond to the submitted request.

- The Staff shall be careful when recording details in documents because those to whom the text refers (such as customers that are individuals) can view this information later. Only appropriate, proportionate, and justified information shall be entered.
- If the Staff receive any request to view Personal Data from other persons (e.g., customers) or any other requests or complaints about the way their Personal Data is processed by the Company, they shall be immediately submitted to the Data Protection Officer, who shall proceed accordingly. There are often strict deadlines for complying with such requests, so any requests shall be submitted as soon as possible after they have been received.

Principle 10: Responsibility

The European data protection legislation requires us to implement a wide range of measures to reduce the risk of violating GDPR and to prove that we take data management seriously. A description of some of the measures we have implemented in order to meet these requirements can be found below.

Records of the Processing Activity

Before GDPR, the data protection authority (the National Supervisory Authority for Personal Data Processing) requested Data Controllers to notify the relevant data protection authority of their processing activities. These obligations are likely to disappear under GDPR. However, we will be required to keep a record of the processing activities involving the personal data which we process. Consequently, the relevant Staff and their team shall ensure that they keep a record of the processing of databases containing personal data. This record shall be made available to the competent supervisory authority, upon request.

Training and Guidance

All Staff members shall read this Policy and shall comply with its terms and conditions. All Staff members who process Personal Data as a significant part of their position shall receive adequate training in terms of data protection and security as part of their induction, and existing Staff members shall receive continuing training.

New Systems and Processes

The European data protection legislation requires us to implement technical and organizational measures to prove that we have considered and integrated the data compliance measures into our processing activities (also known as the principle of data protection by design and by default).

We undertake to comply with this principle by:

- Identifying any confidentiality risks at the start of any project or before implementing a new product, system or service, and planning them accordingly;
- Complying with the principle of data minimization, ensuring that Personal Data are pseudonymized, whenever possible;
- Incorporating confidentiality into our technologies, operations and information architectures and consulting all relevant stakeholders;
- Maintaining the integrity and high standards of our products and services; and
- Striving to be transparent with the individuals regarding the measures taken to protect their Personal Data.

Impact Assessments

If a processing activity is identified as posing a "high risk", a more detailed assessment will be required (a "Data Protection Impact Assessment") before being initiated under GDPR.

The Data Protection Impact Assessment shall include a description of the processing activities, the related risks and the measures taken to mitigate those risks, in particular the protection and security measures taken to protect the Personal Data and to be in line with GDPR. In very limited circumstances, we may be required to consult with the relevant individuals or the relevant data protection authority.

Audit

To prove compliance with the data protection principles and other applicable legal requirements, we shall perform internal audits of our processing activities from time to time. All Staff shall collaborate in the auditing process.

Annex – Safety related Information

Physical Safety

Physical safety is of paramount importance to us and is crucial to ensuring the safety and security of our equipment, as well as the information which our Staff uses or handles.

- At the end of each day, no documents containing Personal Data shall be left on the desk;
- Personal Data shall be kept in a storage cabinet, drawer or locked safe. If it is computerized, it shall be codified, encrypted or password-protected, on both the local hard disk and a network drive that is backed up regularly. If a copy is stored on a removable storage medium, that medium shall be stored in a storage cabinet, drawer, or locked safe.
- Please dispose of any wastepaper safely.
- Please block access to computers on leaving the station.

Data Discovery, Cataloguing and Classification

In addition to the above, we have implemented controls to make sure that Personal Data is properly handled outside of our main systems, including protecting and securing the information, such as:

- Copies of the production databases containing Personal Data made for testing, development or analysis purposes;
- Spreadsheets and other data sources populated by exporting contact details and customer profile information and details of the profile for a mail merge (subject to the same security standard as the main systems);
- Email archives most likely containing Personal Data to be protected under European data protection legislation.

Data Loss Prevention

We control data loss by measures such as automatic blocking of outgoing emails, other messages and movements of files containing Personal Data that have not been protected by appropriate protection measures, *e.g. data encryption.*

In some situations, encryption can be automatically applied to Personal Data when it is classified or identified in an email message or an attachment, whereas, in other situations, the messages can be quarantined to allow for an organizational response.

Data and Email Encryption

Encryption is one of the few specific technologies mentioned in the GDPR text, and its presence basically mandates its use by organizations. We have implemented measures for encrypting data in stand-by and during use or transmission. This ensures that, if a breach occurs in any system, the information remains confidential and GDPR penalties are not triggered.

Identification of a Data Breach and Blocking

The European data protection legislation requires us to report any Personal Data Breach to the competent data protection authority without undue delay (and, whenever

possible, within 72 hours) after learning about that Personal Data Breach (unless it is highly unlikely for it to lead to a risk to the rights and freedoms of the individual). Moreover, it may be necessary to inform individuals in certain cases and we shall document the Personal Data Breach.

Therefore, we have implemented measures to proactively detect any Personal Data Breaches, and look into the size of the event, and create an appropriate organizational response.

- If any individual has information about a Personal Data Breach, he/she shall immediately inform the Data Protection Officer and provide as much information as possible (including the nature and consequences of the Personal Data Breach and any measures taken or proposed to mitigate any adverse effects). Examples of Personal Data Breaches events include sending Personal Data to a wrong recipient, unauthorized access to Personal Data, loss or theft of documents or computers containing Personal Data.

Data Portability

In accordance with art. 20 on the Rights of the data subject, individuals have the right to have their data exported in a usable format that may be given to another provider or service provider to import them into its service in certain circumstances.

Endpoint Security and Mobile Device Management ("MDM")

GDPR requires computing devices to be protected against loss or theft by means of mobile device management capabilities, such as remote *Wipe and Kill*. A lost device could be the weak link in the data protection chain, resulting in a data breach based on information stored on that device or accessible through user credentials that are still active.

Cloud Storage and Sharing Services

The Company carries out a regular review of documents shared to the outside to minimize the degree of sharing with external parties. The use of default restrictions (such as time-bound links) is also encouraged to limit default sharing without the need for user intervention.

- Any transfer of Personal Data shall be performed safely, either externally or internally. When you email or post something, double check that the information is sent to the right recipient.
- Keep in mind that those searching for information sometimes turn to deceit. Before sending any Personal Data to any third party, please verify the identity of that party. This could involve conducting checks to confirm the identity of the third party, especially if you send information by telephone. When in doubt, contact the Data Protection Officer.

Anti-Malware

While a successful infiltration of malware can render computers unusable, one of the more serious concerns raised by GDPR is the potential of malware to recover the credentials for user and administrator accounts. Recovered credentials can then be used

to access the data sources within the organization (both at the headquarters and in cloud services), including those containing personal and sensitive data.

The Company is working closely with its IT service provider to ensure that the highest possible level of security is applied (especially using antivirus and intrusion detection software).

Identity and Access Management
A coherent identity and access management system that easily unifies employees' identity between applications is a fundamental requirement for compliance with GDPR standards. The Company uses the latest identity management protocols, plus user identities are connected to third-party software providers using the *Single Sign-On* option, as the case may be. This ensures that access can be controlled centrally (and quickly) via a series of applications, in a unified way.

***