FIREFLIES

DATA PROCESSING GUIDELINES

DATA PROCESSING GUIDELINES

Through publishing the present data protection guidelines, Swiss Halley AG – hereinafter: Enterprise – fulfills its obligation to provide prior information regarding the processing of the data subjects' personal data, prescribed by Regulation (EU) 2016/679 of the European Parliament and of the Council, in accordance with which, every bit of information according to the respective articles of the Regulation has to be provided to data subjects in a brief, structured, intelligible and accessible form, using a clear and plain language.

I. DATA CONTROLLER INFORMATION

Enterprise informs the data subject that it qualifies as a data controller regarding the processing of their personal data.

COMPANY NAME: Swiss Halley AG
SEAT: 47 Churerstraße, 8808 Pfäffikon, Switzerland
COMPANY REGISTRATION NUMBER: CHE-104.522.189
PHONE: +41 44 508 30 51
COMPANY REPRESENTATIVE: Ulrich Märki
EMAIL: info@firefliestoken.com
WEBSITE: www.firefliestoken.com

DATA PROTECTION OFFICER: Silver Borer
ADDRESS: BC Borer Consulting AG
Seegartenstrasse 2, CH-8008 Zürich
PHONE/FAX: +41 44 254 38 88
EMAIL: dpo@fireflies.com

Personal data are disclosed to the employees of the Enterprise who have the authorization regarding the respective data processing goal and to the persons and organizations that carry out data processing activities for the Enterprise based on service agreements, to the degree defined by the Enterprise and to the extent necessary for carrying out their activities.

II. NAME OF DATA CONTROLLER(S)

(1) The Entrepreneur uses the following data processing entities to carry out its activity. The data processing entities process personal data on the data controller's behalf, exclusively according to the contract created with the Entrepreneur and to the instructions received.

Information technology:

Excite Hungary Kft. (Ltd.)
15/A Vas utca (Street), 1st floor apt. 24, Budapest, H-1088
COMPANY REGISTRATION NUMBER: 01 09 204644
TAX NUMBER: 25183243242

The Enterprise uses outside data-processing entities entrusted with the personal data it processes based on voluntary consent, for the operation and maintenance of its website.

T-Systems Hungary
H-1097 Budapest, Könyves Kálmán körút 36.
Hungary

INTEGRITY Informatics Kft.
H-8000 Székesfehérvár, Gyetvai u. 6.
Hungary

Microsoft Corporation - United States of America

Vertex Wealth Limited
PO Box 227, Peveril Buildings, Peveril Square
IM99 1RZ
Douglas, Isle of Man

Edimi Limited
9a Wick Road Business Park,
Wick Road, Burnham-On-Crouch, Essex, UK, CM0 8LT
Registration number: 11307096

Customer relations tools:

VCC Live Hungary Kft. - Hungary
Monday.com - Israel
LiveChat - United States of America

Marketing tools:

Google LLC (Google Analytics, Google Tag Manager) - United States of America
Facebook Ireland Ltd. - Ireland
Hotjar.com - Malta

Mutual data processing
Swiss Halley AG - Switzerland and Swiss Halley AG Hungarian Commercial Agency - Hungary
Swiss Halley AG - Switzerland and Users of Swiss Halley AG (with regards to the username in the case of product transfer)

Payment providers:
PayU - Poland
Crosscard S.A. - Luxembourg

III. DEFINITIONS

1. "personal data": any 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. "processing": any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3. restriction of processing": the marking of stored personal data with the aim of limiting their processing in the future;

4. "profiling": any form of automated processing of personal data consisting of the use of personal data

to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

5. "pseudonymization": the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

6. "filing system": any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

7. "controller": the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

8. "processor": a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

9. "recipient": a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

10."third party": a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;

11. "consent of the data subject": any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

12. "personal data breach": a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
13. "enterprise": a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

IV. LEGAL BASIS OF THE PROCESSING

1. CONSENT OF THE DATA SUBJECT

(1) Lawfulness of personal data processing has to be based on the data subject's consent or has to have some other legitimate basis, laid down by law.

(2) In case the data processing is based on the data subject's consent, the data subject can provide their consent concerning the processing of their personal data in the following ways:

a) in writing, through a statement giving consent to the processing of personal data b) electronically, through their explicit conduct realized on the Enterprise's website, checking the box, if they perform technical settings regarding this while using information society services, and also through any other statement or act that unambiguously indicates the data subject's consent to the proposed processing of their personal data in the given context.

(3) Silence, pre-ticked boxes or inactivity should not therefore constitute consent.

(4) Consent should cover all processing activities carried out for the same purpose or purposes.

(5) When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(6) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

2. FULFILLMENT OF THE CONTRACT

(1) The processing of data qualifies as lawful if it is necessary for the fulfillment of a contract in which the data subject is one of the parties or in order to take steps at the request of the data subject prior to entering into a contract.

(2) The data subject's consent to personal data processing is not necessary for the fulfillment of the contract, it cannot be a contract requirement.

3. SATISFYING LEGAL OBLIGATIONS APPLYING TO THE CONTROLLER OR PROTECTING THE VITAL INTERESTS OF THE DATA SUBJECT AND OF ANOTHER NATURAL PERSON

(1) The legal basis of data processing is defined by law in the case of fulfilling legal obligations, thus, the data subject is not required to consent to the processing of their personal data.

(2) The controller is obliged to inform the data subject about the purpose, legal basis, duration of the processing, the identity of the controller, about their rights and legal redress option.

(3) Following the withdrawal of the data subject's consent, the controller, under the terms of fulfilling legal obligations, is entitled to process those sets of data that are necessary for the performance of a legal requirement applying to them.

4. PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR IN THE EXERCISE OF OFFICIAL AUTHORITY VESTED IN THE CONTROLLER, ENFORCEMENT OF THE LEGITIMATE INTERESTS PURSUED BY THE CONTROLLER OR BY A THIRD PARTY.

(1) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.

(2) At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.

(3) The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.

V. THE DATA SUBJECT'S RIGHTS IN CONNECTION WITH THE PROCESSING OF THEIR DATA

1. THE ENTERPRISE PROVIDES THE FOLLOWING BRIEF INFORMATION REGARDING THE DATA SUBJECT'S RIGHTS:

The data subject has the right:

a) to receive information prior to the start of data processing,

b) to receive feedback from the controller with regard to whether the processing of their personal data is in progress and if such processing is in progress, they are entitled to gain access to the personal data and the information concerning data processing.

c) to request the rectification, erasure of their data, receive notification from the controller about completing these actions,

d) to request restriction of processing, receive notification from the controller about its completion,

e) to data portability,
f) to object if their personal data is processed for public interest purposes or based on the legitimate interest of the controller.

g) not to be subject to automated decision-making, including profiling

h) to lodge a complaint with the supervisory authority. The data subject can exercise their right to make a complaint via the following channels: Hungarian National Authority for Data Protection and Freedom of Information, address: 22/c Szilágyi Erzsébet fasor, Budapest, H-1125, Phone: +36 (1) 391-1400; Fax:+36(1)391-1410, website: http://www.naih.hu, email: ugyfelszolgalat@naih.hu

i) to effective judicial remedy against a supervisory authority,

j) to effective judicial remedy against the controller or the processor

k) to be informed about personal data breach.

2. DETAILED INFORMATION ABOUT DATA SUBJECT RIGHTS

Right to receive information

(1) The data subject has the right to be informed before the data processing activity starts, concerning information in connection with the processing of their data.

(2) Information to be provided where personal data are collected from the data subject:

a. the identity and the contact details of the controller and, where applicable, of the controller's representative;

b. the contact details of the data protection officer, where applicable;

c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d. where the processing is based on point (f) of Article 6(1) of the Regulation, the legitimate interests pursued by the controller or by a third party;

e. the recipients or categories of recipients of the personal data, if any;

f. where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47 of the Regulation, or the second subparagraph of Article 49(1) of the Regulation, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

(3) In addition to the information referred to in paragraph (1), the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

a. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

c. where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2) of the Regulation, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

d. the right to lodge a complaint with a supervisory authority;

e. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

f. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the Regulation and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(4) Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

a. the identity and the contact details of the controller and, where applicable, of the controller's representative;

b. the contact details of the data protection officer, where applicable;

c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d. the categories of personal data concerned;

e. the recipients or categories of recipients of the personal data, if any;

f. where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1) of the Regulation, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

(5) In addition to the information referred to in paragraph (4), the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

a. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b. where the processing is based on point (f) of Article 6(1) of the Regulation, the legitimate interests pursued by the controller or by a third party;

c. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

d. where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2) of the Regulation, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

e. the right to lodge a complaint with a supervisory authority;

f. from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

g. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the Regulation and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(6) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph (5).

(7) Paragraphs (4) to (6) shall not apply where and insofar as:

a. the data subject already has the information;

b. the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) of the Regulation or in so far as the obligation referred to in paragraph 1 of Article 14 of the Regulation is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

c. obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

d. where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Right of access by the data subject

(1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a. the purposes of the processing;

b. the categories of personal data concerned;

c. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;

d. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such

processing;

f. the right to lodge a complaint with a supervisory authority;

g. where the personal data are not collected from the data subject, any available information as to their source;

h. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the Regulation and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(2) Where personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

(3) The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

THE DATA SUBJECT'S RIGHT TO RECTIFICATION AND ERASURE

Right to rectification

(1) The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure ('right to be forgotten')

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

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 according to point (a) of Article 6(1) of the Regulation, or point (a) of Article 9(2) of the Regulation, and where there is no other legal ground for the processing;

c. the data subject objects to the processing pursuant to Article 21(1) of the Regulation and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the Regulation;

d. the personal data have been unlawfully processed;

e. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

f. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the Regulation.

(2) Where the controller has made the personal data public and is obliged to erase the personal data at the data subject's request, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(3) Paragraphs (1) and (2) 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 reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) of the Regulation as well as Article 9(3) of the Regulation;

d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the Regulation 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 defense of legal claims.

Right to restriction of processing

(1) The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

a. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

b. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;

d. the data subject has objected to processing pursuant to Article 21(1) of the Regulation pending the verification whether the legitimate grounds of the controller override those of the data subject.

(2) Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

(3) A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed

by the controller before the restriction of processing is lifted.

Notification obligation regarding rectification or erasure of personal data or restriction of processing

(1) The controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

(2) The controller shall inform the data subject about those recipients if the data subject requests it.

Right to data portability

(1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

a. the processing is based on consent pursuant to point (a) of Article 6(1) of the Regulation (data subject's consent to the processing of personal data) or point (a) of Article 9(2) of the Regulation (data subject's explicit consent to data processing) or on a contract pursuant to point (b) of Article 6(1); and

b. the processing is carried out by automated means.

(2) In exercising his or her right to data portability pursuant to paragraph (1), the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

(3) The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17 of the Regulation. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

(4) The right referred to in paragraph (1) shall not adversely affect the rights and freedoms of others.

Right to object

(1) The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is carried out in the public interest or in the exercise of official authority or to processing necessary for pursuing the legitimate interests of the controller or by a third party (processing based on point (e) or (f) of Article 6(1) of the Regulation), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

(2) 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, which includes profiling to the extent that it is related to such direct marketing.

(3) Where the data subject objects to processing for direct marketing purposes, the personal data shall

no longer be processed for such purposes.

(4) At the latest at the time of the first communication with the data subject, the right referred to in paragraphs (1) and (2) shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

(5)In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

(6) Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1) of the Regulation, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Right not to be subject to automated decision-making

(1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

(2) Paragraph (1) shall not apply if the decision:

a. is necessary for entering into, or performance of, a contract between the data subject and a data controller;

b. is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

c. is based on the data subject's explicit consent.

(3) In the cases referred to in points a. and c. of paragraph (2), the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

(4) Decisions referred to in paragraph (2) shall not be based on special categories of personal data referred to in Article 9(1) of the Regulation, unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

DATA SUBJECT'S RIGHT TO LODGE A COMPLAINT AND TO JUDICIAL REMEDY

Right to lodge a complaint with a supervisory authority.

(1) Based on Article 77 of the Regulation, the data subject has the right to lodge a complaint with the supervisory authority if, according to the data subject's judgement, the processing of personal data relating to them infringes this Regulation.

(2) The data subject can exercise their right to lodge a complaint via the following channels: Hungarian National Authority for Data Protection and Freedom of Information, address: 22/c Szilágyi Erzsébet

fasor, Budapest, H-1125, Phone: +36 (1) 391-1400; Fax:+36(1)391-1410, website: http://www.naih.hu, email: ugyfelszolgalat@naih.hu

(3) The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78 of the Regulation.

Right to an effective judicial remedy against a supervisory authority

(1) Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

(2) Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77 of the Regulation.

(3) Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

(4) Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court

Right to an effective judicial remedy against a controller or processor

(1) Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77 of the Regulation, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

(2) Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Restrictions

(1) Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in the Regulation, in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

a. national security;

b. defense;

c. public security;

d. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

e. other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

f. the protection of judicial independence and judicial proceedings;

g. the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

h. a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

i. the protection of the data subject or the rights and freedoms of others;

j. the enforcement of civil law claims.

(2) In particular, any legislative measure referred to in paragraph (1) shall contain specific provisions at least, where relevant, as to:

a. the purposes of the processing or categories of processing;

b. the categories of personal data;

c. the scope of the restrictions introduced;

d. the safeguards to prevent abuse or unlawful access or transfer;

e. the specification of the controller or categories of controllers;

f. the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
g. the risks to the rights and freedoms of data subjects; and

h. the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

Communication of a personal data breach

(1) When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

(2) The communication to the data subject referred to in paragraph (1) of this Article shall describe in clear

and plain language the nature of the personal data breach and contain at least the name and contact details of the data protection officer or another contact person capable of providing further information, the likely consequences resulting from the personal data breach, measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate possible adverse effects of the personal data breach.

(3) The communication to the data subject referred to in paragraph (1) shall not be required if any of the following conditions are met:

a. the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;

b. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph (1) is no longer likely to materialize;

c. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

(4) If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph (3) are met.

VI. PROCEDURE APPLICABLE AT THE DATA SUBJECT'S REQUEST

(1) The Enterprise assists the data subject in exercising their rights, it cannot deny the fulfillment of the data subject's request regarding the exercise of their rights stated also in the present data processing guidelines, unless it proves that it cannot identify the data subject.

(2) The Enterprise provides information on actions taken regarding the request to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

(3) Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

(4) If the Enterprise does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

(5) The Enterprise provides the data subject with the following information and actions free of charge: feedback about the processing of personal data, access to the processed data, data rectification, completion, erasure, restriction of processing, data portability, objection to data processing, communication of personal data breach.

(6) Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller, considering the administrative expenses entailed by the requested information or communication or taking the requested measures, may: charge EUR 50, or refuse to take action on the request.

(7) The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

(8) Without prejudice to Article 11 of the Regulation, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21 of the Regulation, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

VII. PROCEDURE FOR PERSONAL DATA BREACH

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

(2) The losing or stealing of the device containing personal data (laptop, mobile phone) qualifies as personal data breach, furthermore, losing the code necessary for the decryption of the set of data encrypted by the controller, this code becoming inaccessible, infection with ransomware (extortion virus), which makes the data processed by the controller inaccessible until the ransom is paid, attacks on the information technology system, emails containing personal data sent by mistake, making the list of addresses public etc. also qualifies as personal data breach.

(3) In case personal data breach is noticed, the Enterprise's representative immediately carries out an investigation in order to identify the personal data breach and assess the possible consequences. Necessary actions have to be taken to avert the damage.

(4) It should notify the supervisory authority about the personal data breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons justifying the delay should also be enclosed.

(5) The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

(6) The notification referred to in paragraph (4) shall at least:

a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c. describe the likely consequences of the personal data breach;

d. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(7) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

(8) The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with Article 33 of the Regulation.

VIII. DATA PROCESSING RELATED TO THE WEBSITE

Information related to the data of the visitors of the Enterprise's website

(1) When the Enterprise's website is visited, one or more cookies - tiny information package sent by the server to the browser, then, sent back to the server by the browser every time a request is made to the server – are sent to the computer of the person visiting the website, through this/these, their browser becomes uniquely identifiable in case the person visiting the website provides their explicit (active) consent to this through their conduct aimed at continuing to browse the website, after receiving clear and unambiguous information.

(2) Cookies are used exclusively to improve user experience, make the sign-in process automatic. Cookies used by the website do not store information suitable for personal identification, the Enterprise does not carry out personal data processing in this respect.

(3) The range of processed data when the Enterprise's website is visited: IP address, operation system, browser.

(4) The duration of data processing when the Enterprise's website is visited: until the withdrawal of the consent provided by the concerned party, or otherwise, 90 days after leaving the website.

(5) If someone registers an account on firefliestoken.com, a Fireflies profile will automatically be created for them using the same information.

Registration, newsletter subscription

(1) The legal basis of the data processing, in the case of registration, newsletter subscription, is the data subject's consent, this is provided by the data subject through checking the box next to the texts "registration" and "newsletter subscription" on the Enterprise's website, after receiving information about the processing of their data.

(2) The set of data subjects for registration, newsletter subscription: every natural person who wishes to subscribe to the Enterprise's newsletter or wishes to register at the website and consents to the processing of their personal data.

(3) The set of processed data in the case of newsletter subscription: name, email address.

(4) The range of processed data for registration: username, email address, country, the individual identification number provided by the Enterprise (user ID).

(5) The purpose of data processing in the case of newsletter subscription: providing the data subject with information about the Enterprise's services, products, about changes occurred concerning these, communicating news, events.

(6) The purpose of data processing in the case of registration: communication for contract preparation purposes, providing the data subject with services available at the website free of charge, access to non-public website content.

(7) Data recipients (to whom the data can be disclosed) in the case of newsletter subscription, registration: the head of the Enterprise, customer relations employee, employees working for the data processor responsible for operating the Enterprise's website.

(8) Data processing period in the case of newsletter subscription, registration: in the case of newsletter subscription, until unsubscribing, in the case of registration, until cancellation at the data subject's request.

(9) At any time, the data subject can unsubscribe from the newsletter and request the cancellation of their registration (erasure of their personal data). Unsubscribing from the newsletter is carried out by clicking on the unsubscribe link in the footer of the emails sent to the data subject or by a letter sent to the Enterprise's seat.

Data processing in connection with direct marketing activity

(1) The legal basis of the Enterprise's data processing for direct marketing purposes is the data subject's consent that is unambiguous and explicit. The data subject provides their unambiguous, explicit prior consent on the Enterprise's website, by checking the box next to the text concerning consent to direct marketing communication, after receiving information about the processing of their data.

(2) The data subject can also provide their consent in paper format, by completing the form constituting Appendix 2 of the present guidelines.

(3) The set of data subjects: every natural person who gives their unambiguous, explicit consent to the processing of their personal data for direct marketing purposes by the Enterprise.

(4) Purposes of data processing: sending advertisements, offers related to providing services, product sales, communication of promotions electronically or by post.

(5) Personal data recipients: the head of the Enterprise, employees carrying out customer service tasks, marketing tasks based on their duties.

(6) The set of personal data processed: name, address, phone number, email address.

(7) Data processing period: until the processing of personal data for direct marketing purposes is withdrawn by the data subject.

Data processing related to the webshop

(1) The above clauses apply to webshop registration, to data processing activity related to newsletter subscriptions and to informing the visitors.

(2) Contracts created online, electronically, on the Enterprise's website (purchases) render necessary the fulfillment of the requirements laid down by the laws effective at the sale's location, thus, the purposes of data processing, in addition to the above mentioned, are demonstrating the fact that the service provider's obligation of informing the consumers, prescribed by the act, is fulfilled, verifying that the contract has been created, creating the contract, defining and modifying its content, monitoring its fulfillment, billing concerning the fee(s) it entails and enforcing the claims related to it.

(3) In case a search, purchase, or product transfer is carried out at the webshop, the legal basis of data processing is the fulfillment of the contract, that of legal obligations.

(4) Data categories concerned by data processing:

During search: IP address, the unique search ID, search information (date, place, etc.).

During purchase: name, date of birth, place of birth, citizenship, address, phone number, identity card number, passport number, age, bank account number (in certain refund cases), booking or purchase information.

Regarding product transfer: username.

(5) Categories of data subjects concerned by processing: every natural person who registers at the Enterprise's webshop, subscribes to the newsletter, search, makes purchases.

(6) Categories of data recipients: the head of the Enterprise, employees carrying out customer relations tasks, sales-related tasks, the employees of the data processor carrying out the operation of the Enterprise's website and the Enterprise's employees carrying out accounting tasks, employees of the data processor carrying out these tasks.

(7) Swiss Halley AG may share the user's data with third parties that provide services to the user on Swiss Halley AG's behalf.
All third-party service providers are required to take the security measures in line with Swiss Halley AG's policies in order to protect your data. Swiss Halley AG does not allow third parties to use the user's data for their own purposes. Swiss Halley AG gives permission to process the user's data only for specified purposes and in accordance with Swiss Halley AG's instructions.
Swiss Halley AG does not share more data than the minimum amount necessary.

(8) The data processing venue is the seat of the Enterprise.

(9) Data processing period:

Regarding searches: 3 years following the end date of the service reserved or used (e.g. the check-out date for accommodation reservations, the arrival date for flight ticket purchases), or otherwise, 3 years following the search. During the 3-year period, the concerned party can request the restriction of data processing.

Regarding purchases and transfers, 10 years after the purchase, use, or transfer.

During the 10-year period, the concerned party can request the restriction of data processing.

IX. DATA PROCESSING ACTIVITY RELATED TO THE FULFILLMENT OF THE CONTRACT

(1) The Enterprise processes the personal data of those natural persons – clients, customers, suppliers – with whom it enters into a contract, in relation to the contractual relationship. The data subject should be informed about the processing of personal data.

(2) The set of data subjects: every natural person who enters into a contract with the Enterprise.

(3) The legal basis of data processing is the fulfillment of the contract, the purposes of data processing are communication, pursuing claims created through the contract, ensuring that contractual obligations are fulfilled.

(4) Personal data recipients: the head of the Enterprise, employees, data processors of the Enterprise carrying out customer service, accounting tasks based on their duties.

(5) (5) Swiss Halley AG can share the user's data with third parties that provide services to the user on Swiss Halley AG's behalf.

Every third party providing its service is obliged to take the security measures following Swiss Halley AG's requirements in order to protect their data. Swiss Halley AG does not allow third parties to use the user's data for their private purposes.

Swiss Halley AG permits the processing of the user's data exclusively in accordance with its instructions and for predefined purposes. Swiss Halley AG does not share more data than the necessary minimum.

(6) The range of the processed personal data: name, username, date of birth, place of birth, citizenship, address, phone number, identity card number, passport number, age, ePayments ID, bank account number (in certain refund cases), booking or purchase information, report information for administrative tasks.

(7) Duration of data processing:

> 10 years after the purchase, the use of the product or service, the transfer of the product, or other payments.
>
> Regarding administrative tasks, 10 years after the administrative task is closed, or the service or the product is used (whichever comes last).
>
> During the 10-year period, the concerned party can request the restriction of data processing.

X. PROVISIONS CONCERNING DATA SECURITY

(1) The Enterprise can process personal data only in accordance with the activities stated in the present guidelines, according to the purpose of data processing.

(2) The Enterprise takes care about data security, in this respect, it is obliged to take all technical and organizational measures that are essential for the implementation of data security rules, data protection and confidentiality rules, and creates the procedure rules necessary for the implementation of the above

stated statutes.

(3) Taking the appropriate measures, the Enterprise protects the data from unlawful access, modification, forwarding, disclosure, erasure or destruction, and from accidental destruction and damage, in addition, from inaccessibility resulting from any change in the applied technology.

(4) The Enterprise's "Data protection guidelines" contains the technical and organizational measures the Enterprise should take to ensure data security.

(5) When defining and applying data security measures, the Enterprise considers the all-time developmental level of technology, in case more data processing options are available, it chooses the solution that provides higher personal data protection unless it involves disproportionate effort.

XI. RULES RELATED TO DATA PROCESSING

1. GENERAL RULES RELATED TO DATA PROCESSING

(1) The data processor's rights and obligations related to personal data processing are defined by the law and, within the framework of separate statutes concerning data processing, by the controller.

(2) The Enterprise declares that it does not have substantial decision-making competency concerning data processing in the course of the data processor's activity, it can process the personal data it becomes aware of exclusively according to the rules defined by the controller, it cannot process data for its own account, furthermore, it is obliged to store and maintain the personal data according to the conditions set forth by the controller.

(3) The Enterprise is responsible for the lawfulness of data processing operation instructions given to the data processor.

(4) The Enterprise is obliged to inform the data subjects about the data processor's identity, the data processing venue.
(5) The Enterprise allows the data processor to employ further data processors.

(6) The contract concerning data processing has to be in writing. Data processing tasks cannot be assigned to organizations that are interested in business activities using the personal data under processing.

Date: February 05, 2024
(updated on November 26, 2024)