May 25, 2018

SZENTKIRÁLYI-KÉKKÚTI ÁSVÁNYVÍZ TERMELŐ ÉS FORGALMAZÓ KFT.

DATA PROTECTION POLICY

179887v8

TABLE OF CONTENTS

1. GENERAL TERMS AND CONDITIONS 4

2. THE SCOPE OF PERSONAL DATA AND INFORMATION SUBJECT TO THE DATA CONTROLLING PROCESS AND THE LEGAL GROUNDS, THE PURPOSE AND THE DURATION OF SUCH PROCESS 6

3. THE PRECEPTS AND THE METHOD OF THE DATA CONTROLLING PROCESS 15

4. FORWARDING PERSONAL DATA AND INFORMATION 16

5. DATA PROCESSORS 17

6. PARTIES HOLDING ACCESS TO PERSONAL DATA AND INFORMATION 17

7. THE ARCHIVAL AND SECURITY OF PERSONAL DATA AND INFORMATION 18

8. PROCEDURES TO FOLLOW IN THE CASE OF DATA BREACHES 19

9. DATA SECURITY OFFCER 19

10. IMPACT ASSESSMENT OF DATA SECURITY 19

11. EFFACEMENT OF PERSONAL DATA AND INFORMATION 20

12. THE DATA SUBJECTS' RIGHTS AND THEIR ENFORCEMENT 20

13. ALTERNATIVES OF THE ENFORCEMENT OF RIGHTS 22

14. MODIFICATION OF THIS DATA PROTECTION POLICY 23

APPENDIX 1 Data Processors 24

APPENDIX 2 Data Privacy Notes 26

PART 1 26

Data Privacy Note for Applicants (in the Script of Advertisements of Vacancies) 26

PART 2 26

Data Privacy Note for Applicants Refused (Request for Consent) 26

PART 3 26

Data Privacy Note for Employees (to be Circulated and Undersigned as an Appendix to be attached to the Contracts of Employment) 26

PART 4 29

Data Privacy Note included in Contracts concluded with Suppliers/Vendors 29

PART 5 30

Consent to the Delivery and Acceptance of Promotional Presents 30

PART 6 30

Data Controlling Notes connected with Personal Data and Information Controlled and Processed in the course of Direct Marketing communicated to Consumers 30

PART 7 31

Note of the Use of Cookies on the Websites 31

PART 8 32

Information regarding Monitoring and Surveillance by Global Positioning System (GPS) 32

PART 9 32

Information regarding Camera Surveillance 32

APPENDIX 3 34

Specific Directions of the Operation of the Security Camera Surveillance System 34

APPENDIX 4 36

Data Forwarding File 36

APPENDIX 5 37

Data and Information Security Measures 37

APPENDIX 6 40

Data Breach Report 40

1. GENERAL TERMS AND CONDITIONS

1.1 The Objective of this Data Protection Policy

The objective of this Data Protection Policy (hereinafter referred to as "**Policy**") is to incorporate particular data protection and data controlling precepts applied by the Szentkirályi-Kékkúti Ásványvíz Termelő és Forgalmazó Kft. (as "**Data Controller**" OR "**Szentkirályi-Kékkúti**") and to set forth Data Controller's Data Protection and Data Controlling Policy by which the Szentkirályi-Kékkúti Ásványvíz Termelő és Forgalmazó Kft. as Data Controller shall be bound.

While setting forth the provisions of this Policy, Data Controller attentively respected the content of regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation; for the purpose of this Policy: "**GDPR**") and the statutory provisions of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as "Information Act"; for the purpose of this Policy: "**Infotv.**") as well as other provisos in effect.

According to Art. 30 of the GDPR, Data Controller is responsible for executing the files and archives of all relevant Data Controlling Processes updated. Such obligation is observed by executing this Policy updated and whatsoever modified and/or amended if necessary.

1.2 Definitions

For the purpose of entering this Policy into effect, the terms below shall be construed as follows:

1.2.1 **Data or Personal Data**: any and all data and information by which a natural person ("**Data Subject**") can be identified, either directly or indirectly.

1.2.2 **Data Processor**: any and all service providers that are assigned to process Personal Data and Information on behalf of Data Controller. In view of the Services referred to in this Policy, Data Processors shall be the entities defined therein.

1.2.3 **Data Controlling Process**: irrespective of the process applied, any and all operations, actions, measures and undertakings connected with all Personal Data and Information, principally their collection, recording, systematization, segmentization, archival, conversion, modification, application, querying, examination, disclosure, forwarding, circulation or any other method of access to them, as well as their dissemination, harmonization, connection, restriction, omission or annihilation.

1.2.4 **Data Controlling Note** OR **Note**: any and all written or recorded texts or scripts whose purpose is to properly inform all Data Subjects of the controlling of their Personal Data and Information, including the legal basis, the purpose and the duration of the Data Controlling Process as well as the rights of the Data Subjects.

1.2.5 **Data Controller**: entity that, either solely or conjointly, is eligible to define the purposes and methods of the Data Controlling Process. In view of the Services referred to in this Policy, the following entity shall be regarded as Data Controller:

Denomination	Szentkirályi-Kékkúti Ásványvíz Termelő és Forgalmazó Korlátolt Felelősségű Társaság
Incorporation code	Cg.01-09-717667
Taxation code	13079026-2-44
Business domicile	H-1117 Budapest, Neumann János u. 1. 1. em.
Contact person	Dr. Balázs Szabó
Telephone number	+36/80/200-329
E-mail:	adatvedelem@szentkiralyi-kekkuti.hu, leiratkozas@szentkiralyi-kekkuti.hu (for the purpose of data erasure)
Website	www.szentkiralyi.hu, www.theodora.hu

1.2.6 **Data Breach:** any and all security breaches in consequence of which any and all Personal Data and Information, either forwarded, archived or whatsoever controlled by any method, have been annihilated, forfeited, modified, illicitly disclosed or accessed, either unintentionally or illicitly.

1.2.1 **Add-ons/Extensions**: Add-ons/extensions, such as "Like", "Share" or "Follow", etc. and the icon of the Social Media page operated by Social Media.

1.2.2 **Customized Data Controlling Policy:** particular Customized Data Controlling Policies applied by Szentkirályi-Kékkúti in the scope of marketing.

1.2.3 **Ekertv.**: Act CVIII of 2001 on certain issues of electronic commerce activities and information society services.

1.2.4 **Data Subject**: any natural person, either identified OR identifiable.

1.2.5 **Websites**: the following websites:

www.theodora.hu
www.theodora-info.hu
www.nestle-aquarel.hu
www.kekkuti.hu
www.kekkuti.eu
www.theodora.eu
www.kekkutiasvanyvizrt.hu
www.theodoraquelle.hu
www.magnesia.hu

www.theodorajatek.hu
https://szentkiralyinyeremeny.hu

1.2.6 **GDPR:** regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

1.2.7 **Infotv:** Act CXII of 2011 on informational self-determination and freedom of information.

1.2.8 **KMV Group:** Karlovarské Minerální Vody, a.s. (business domicile: Horova 3360 21 Karlovy Vary, the Czech Republic; incorporation code: 14706725) and Central Europe Mineral Water Holding (business domicile: Mariánské náměstí 159/4, Staré Město, 110 00 Prague 1; the Czech Republic; incorporation code: 038 60 817) conjointly.

1.2.9 **Social Media and Network:** Facebook, Instagram, Twitter; LinkedIn, etc.

1.2.10 **Public Archives Act**: Act LXVI of 1995 on public records, public archives and the protection of private archives.

1.2.11 **Marketing Act**: Act CXIX of 1995 on the handling of names and addresses used for the purpose of market research and direct business dealing.

1.2.12 **Mt.**: Act I of 2012 on the [Hungarian] Labor Code.

1.2.13 **Employees/Staff:** any and all natural persons employed by Data Controller.

1.2.14 **NAIH**: Hungarian National Authority for Data Protection and Freedom of Information.

1.2.15 **Ptk.:** Act V of 2013 on the [Hungarian] Civil Code.

1.2.16 **Data Protection Policy:** Data Controller's current Data Protection Policy.

1.2.17 **Personal and Property Security Act:** Act CXXXIII of 2005 on the statutory provisions of personal and property security as well as private detective operations.

1.2.18 **Szentkirályi-Kékkúti** as Data Controller.

Any term NOT governed hereabove shall be construed in concert with the statutory provisions set forth in the Infotv. and the GDPR.

2. THE SCOPE OF PERSONAL DATA AND INFORMATION SUBJECT TO THE DATA CONTROLLING PROCESS AND THE LEGAL GROUNDS, THE PURPOSE AND THE DURATION OF SUCH PROCESS

The following personal data and information will be controlled, managed and handled by Data Controller according to the following legal grounds and for the purpose and duration set forth herebelow:

2.1 The personal data and information of applicants applying for vacancies (applications NOT evaluated yet)

2.1.1 Legal grounds:

The Data Controlling Process is required for the enforcement of the licit interests of Data Controller in full conformity with the content set forth in Section **Error! Reference source not found.** herebelow (Art. 6 (1) (f) of GDPR).

2.1.2 The scope of Personal Data and Information subject to the Data Controlling Process and the purpose of such process:

TYPES OF PERSONAL DATA & INFORMATION	PURPOSE OF THE DATA CONTROLLING PROCESS
Name, e-mail address, telephone number, occasionally address, data and information included in applications (CVs) for vacancies	To implement the application procedure properly (licit interest)

2.1.1 Method of information for Data Subjects: the Note in PART 1 of APPENDIX 2 [part 1] will be inserted into the scripts of advertisements of vacancies.

2.1.2 The duration of the Data Controlling Process: until the end of the evaluation of applications for vacancies, except if data and information should be processed according to Section 2.2 OR 2.3.

2.2 The personal data and information of applicants applying for vacancies (refused applications)

2.2.1 Legal grounds:

Data Subjects have consented to the Data Controlling Process of their personal data and information for one or more concrete purposes (Art. 6 (1) (a) of GDPR).

2.2.2 The scope of Personal Data and Information subject to the Data Controlling Process and the purpose of such process:

TYPES OF PERSONAL DATA & INFORMATION	PURPOSE OF THE DATA CONTROLLING PROCESS
CVs and all data and information contained therein	To notify Data Subjects of potential vacancies in the future (consent)

2.2.3 Method of information for Data Subjects: by inserting the script of the Note set forth in PART 2 of APPENDIX 2 [part 2] in e-mails.

2.2.4 The duration of the Data Controlling Process: until the rescindment of the consent. Such consent can be rescinded by an application to be delivered to the contacts defined in Section 1.2.5 above defined by Data Controller.

2.3 The personal data and information of Employees (current Employees)

2.3.1 Legal grounds:

(a) The Data Controlling Process is required for the consummation of a contract in which the Data Subject is one of the parties (Art. 6 (1) (b) of GDPR);

(b) The Data Controlling Process is required for the consummation of a legal obligation anent Data Controller (Art. 6 (1) (c) of GDPR), whereas such legal obligation is grounded on Section 51(4) of the [Hungarian] Labor Code, on Section 3 of Appendix 1 of Act CL of 2017 on taxation, on Sections 79(1), 80(1) of Act LXXX of 1997 on the eligibility for social security benefits and private pensions and the funding for these services, and on Section 46(2) of the corresponding law;

(c) The Data Controlling Process is required for the enforcement of the licit interests of Data Controller (Art. 6 (1) (f) of GDPR).

2.3.2 The scope of Personal Data and Information subject to the Data Controlling Process and the purpose of such process:

TYPES OF PERSONAL DATA & INFORMATION	PURPOSE OF THE DATA CONTROLLING PROCESS
Full name, name at birth, mother's maiden name, place and date of birth, taxation number, social security number, bank account number, permanent and/or temporary address/residence, ID Card number, documents of termination of employment from previous job/workplace, information regarding child support, monthly remittance(s) subject to adjudication(s) by any court of law, attendance report, report of medical checkup by occupational physician, personal data and information connected with occupational accident(s), sizes of footwear and gear (for work wear), record of employment, data and information included in contract of employment	To comply with contract of employment properly, including payroll (to abide by the contract)
Data and information stipulated by Section 3 of Appendix 1 of Act CL of 2017 on taxation	Taxation norms, reporting employment (stipulation by law)
Data and information stipulated by Sections 79(1), 80(1) of Act LXXX of 1997 on the eligibility for social security benefits and	For the purpose of data service of health care nature (stipulation by law)

private pensions and the funding for these services	
Data and information stipulated by Section 46(2) Act LXXX of 1997 on the eligibility for social security benefits and private pensions and the funding for these services	For the purpose of data service of social security nature (stipulation by law)
Report of annual medical checkup by occupational physician (Data Controller is only entitled to learn the result, either "capable" or "incapable", as evaluated by the physician and is unentitled to acquire access to underlying medical data and information)	To abide by the content set forth in the [Hungarian] Labor Code (stipulation by law)
Full name and address/residence	To circulate Monthly Bulletin (monthly newspaper) (licit interest)
Full name and sizes of gear	To order work wear and free gear as present (licit interest)
Access/entry card: by using the card in order to record access/entry to, leaving from and time spent out of site on workdays; date of receipt, date of card activation, serial number of card, date of returning card; full name, occupation, position, entitlement of access/entry, serial number of card	To check real performance at work place during working hours (licit interest)

2.3.3 Method of information for Data Subjects: rendered as part of a discrete instruction on the day of the execution of the contract of employment, the Data Privacy Note in PART 3 of APPENDIX 2 [part 3], which must be read, construed, understood and undersigned by Employees, will be used for this purpose.

2.3.4 The duration of the Data Controlling Process:

(a) should the completion of the contract be the legal grounds of the Data Controlling Process:

- as long as required by the completion of the contract;
- subsequent to the termination of the effect of the contract: further period of 3 (three) years for the purpose of enforcement of contingent legal claims pursuant to Par. 286 of the [Hungarian] Labor Code (in such a case, the Data Controlling Process will take place on the basis of the licit business interest of Data Controller to the extent necessary);

(b) should the adherence to legal obligations binding the Data Controller be the legal grounds of the Data Controlling Process: as long as being mandatory for the employment of the concerned Employee on the basis of the effective laws, except data and information that are disallowed to be erased for the purpose of exercising the rights of the Data Subjects pursuant to Item j) of Par. 3 and Par. 4 of the Public Archives Act;

(c) should the enforcement of the licit business interest of Employer be the legal grounds of the Data Controlling Process: as long as the Data Controlling Process is required for the enforcement of the licit interest of Employer, except if (i) the Data Subjects' fundamental rights and freedom connected with the protection of Personal Data and Information have been privileged over such an interest; OR (ii) the Employees refuse the Data Controlling Process, and Employer is unable to verify that its licit business interest should be privileged over the Employees' interests.

(d) As regards access/entry cards, the dates/times of entry/access and leave will be effaced after 6 (six) months. Moreover, upon termination of the effect of employment, all personal data and information controlled, managed and handled in connection with such cards will be deleted.

2.4 The personal data and information of suppliers (subcontractors) and business clientele

2.4.1 Legal grounds:

(a) The Data Controlling Process is required for the enforcement of the licit interest of Data Controller (Art. 6 (1) (f) of GDPR);

(b) The Data Controlling Process is required for the consummation of a contract in which the Data Subject is one of the parties (Art. 6 (1) (b) of GDPR);

(c) The Data Subjects have consented to the Data Controlling Process of their personal data and information for one of more concrete purposes (Art. 6 (1) (a) of GDPR).

2.4.2 The scope of Personal Data and Information subject to the Data Controlling Process and the purpose of such process:

TYPES OF PERSONAL DATA & INFORMATION	PURPOSE OF THE DATA CONTROLLING PROCESS
Full name, address, taxation number, name of person as representative (in the case of legal entities and contracting parties), e-mail address	Information required for liaison (licit interest, execution of contract in the case of a contract concluded with a natural person)
Sizes of gear (in the case presents for promotion)	To evaluate needs for the manufacturing of customized equipment, to organize deliveries, to dispatch Christmas presents, to

	invite for tenders, to request for quotations, to hand presents of incentive programs (consent)

2.4.3 Method of information for Data Subjects:

(a) should the Data Controlling Process be grounded on the licit interests of Data Controller: via the Data and Information Security passage set forth in the contract according to PART 4 of APPENDIX 2 [

(b)

(c)

(d) PART 4].

(e) should the Data Controlling Process be grounded on consent: in the script attached to the receipts undersigned upon the delivery of presents according to PART 5 of APPENDIX 2 [PART 5].

2.4.4 The duration of the Data Controlling Process:

(a) should the completion of the contract be the legal grounds of the Data Controlling Process: for 5 (five) years subsequent to the termination of the effect of the given contract, if the Data Subjects do not object to it, and it is unverifiable whether the Data Controller's licit interests are privileged over those of the Data Subjects;

(b) should consent be the legal grounds of the Data Controlling Process: until the rescindment of the consent.

2.5 The personal data and information of the Data Subjects in the course of marketing campaigns

2.5.1 Legal grounds:

(a) The Data Subjects have consented to the Data Controlling Process of their personal data and information for one or more concrete purposes (Art. 6 (1) (a) of GDPR). Szentkirályi-Kékkúti is not to control, handle or manage the personal data and information of minors under the age of 16 in the course of any marketing activity and to exert reasonable efforts to monitor such minors so as not to take part in such marketing campaigns. Measures to be undertaken by Szentkirályi-Kékkúti in this respect, depending on the nature of the Data Controlling Processes:

(i) as regards own developed platforms, registration is required for the participation in campaigns, where the participants are required to indicate their dates of birth, based on which the system will disqualify minors under the age of 16;

(ii) if the campaign/promotion is run on any social media platform, the customized setting of the participants decides whether the age of the Data Subjects can be seen, based on which the participants cannot be selected, and the rules stipulate that the campaign/promotion is pertained to participants over the age of 16;

(iii) as regards campaigns/promotions run on the basis of personal contact, the hostess is to ensure that all participants are over the age of 16.

(b) The Data Controlling Process is required for the enforcement of the licit interests of Data Controller (Art. 6 (1) (f) of GDPR).

2.5.2 The scope of Personal Data and Information subject to the Data Controlling Process and the purpose of such process

TYPES OF PERSONAL DATA & INFORMATION	PURPOSE OF THE DATA CONTROLLING PROCESS
Full name; date of birth; telephone number; address/residence (city, street, ZIP Code), e-mail address.	To circulate newsletters, direct marketing
Users that like, follow and make comments about the Social Websites of Data Controller, the data of all profiles (e.g.: name, e-mail, address, photograph, comments, evaluations, etc.) published by them, IP address, e-mail address, hostess activity information (receipts of presents, information required for mail delivery of prizes in the case of winning players), name, telephone number, e-mail address, date of shopping, AP Code of shopping receipt, optionally preferences to presents (e.g.: selecting color, city), optionally size of gear (if not unisex and presents are available in varying sizes), signature	To ensure contact, to maintain contact, participation in events, promotions, raffles and sweepstakes, and to notify winners
IP address (automatic recording), demographic data, browsing history (via cookies)	To improve and ensure high quality of services rendered by the Websites (licit interest)
Demographic data of visitors (age, spoken language, country, age, etc.) visiting the Websites	To know more of the visitors visiting the Websites (licit interest)

2.5.3 Method of information for Data Subjects:

(a) in the case of newsletters and direct marketing, the Note, whose script is incorporated in PART 6 of APPENDIX 2 [PART 6

(b)], published on the particular interface;

(c) in the case of events, the Note, whose script is incorporated in PART 6 of APPENDIX 2 [PART 6

(d)], published on the particular Website or on the Facebook page of the particular event;

(e) in the case of raffles and sweepstakes, the Note, whose script is incorporated in PART 6 of APPENDIX 2 [PART 6

(f)], published on the particular Website and/or on the Social Media pages of the Szentkirályi-Kékkúti;

(g) in the case of Add-ons/Extensions applied by Social Media, the Note, whose script is incorporated in PART 6 of APPENDIX 2 [PART 6

(h)], that which is to be composed in accordance with the actual method of publication;

(i) in the case of the application of cookies, the Note, whose script is incorporated in PART 7 of APPENDIX 2 [PART 7], inserted in the field which automatically pops up, when the particular Website is visited.

2.5.4 The duration of the Data Controlling Process:

(a) in the case of newsletters and direct marketing: until rescindment of the consent;

(b) in the case of events, raffles and sweepstakes: as long as required by the completion of the event and until the announcement of the winner in the case of raffles and sweepstakes.

(c) in the case of the application of Add-ons/Extensions operated by Social Media and in the case of users' comments made on the Social Media of the Szentkirályi-Kékkúti: data and information may be used until rescindment (request for effacement, or the Data Subjects no longer follow the page and delete their comments);

(d) in the case of the application of cookies: data and information carried by cookies may be used until the moment the Data Subjects disable the use of cookies in the browsing setting, and until the Data Controlling Process is necessary for the technical operation of the Website at latest.

2.5.5 Presence on Social Media and the controlling process of data and information obtained by placing Add-ons/Extensions operated by Social Media on the Websites are realized on the Social Media, so that the general terms and conditions of the particular Social Media will apply to the erasure and modification of such data and information.

2.6 Data Controlling Process regarding the data and information of parties physically entering the office premises and bottling plants of Data Controller by security camera surveillance

2.6.1 Legal grounds:

The Data Controlling Process is required for the enforcement of the licit interest of Data Controller (Art. 6 (1) (f) of GDPR) according to the content set forth in Section 2.6.2 herebelow:

2.6.2 The scope of Personal Data and Information subject to the Data Controlling Process and the purpose of such process

TYPES OF PERSONAL DATA & INFORMATION	PURPOSE OF THE DATA CONTROLLING PROCESS
Images and visuals recorded by video cameras	To safeguard personal and property security as well as public health conditions and public security/safety (licit interest)

2.6.3 Method of information for Data Subjects: Data Controlling Note to be displayed before sites/areas that are under camera surveillance. The script of the Note is encompassed in PART 9 of APPENDIX 2 [PART 8].

2.6.4 The duration of the Data Controlling Process (3 (three) work days / 30 (thirty) work days in legal harmony with Article (2) of Par. 31 of the Personal and Property Security Act), except if the Personal Data and Information are to be used as exhibits in the course of any court proceeding in full conformity with Article (5) of Par. 31 of the Personal and Property Security Act.

2.6.5 The specific directions of the operation of the security camera surveillance system are set forth in APPENDIX 3[**Error! Reference source not found.**] below.

2.7 Tracking Employees by GPS navigation system

2.7.1 Legal grounds:

The Data Controlling Process is required for the enforcement of the licit interest of Data Controller (Art. 6 (1) (f) of GDPR)).

2.7.2 The scope of Personal Data and Information subject to the Data Controlling Process and the purpose of such process

TYPES OF PERSONAL DATA & INFORMATION	PURPOSE OF THE DATA CONTROLLING PROCESS
Mileage records of corporate vehicles used by Employees and the data of the GPS navigation	To organize particular work processes accurately, to check the

system (showing the actual location and velocity of the vehicles on the map, showing the route of the vehicles on the map retrospectively, showing the motions of the vehicles (starting and stopping positions, mileages/kilometers, runtime, idle time, average velocity))	loci of Employees that drive en route to defined destination (licit interest)

2.7.3 Method of information for Data Subjects: Data Controlling Note in the Manual of Operation to be provided with any and all Employees that use corporate vehicles prior to such use. The script of the Note is encompassed in PART 8 of APPENDIX 2 [PART 8].

2.7.4 The duration of the Data Controlling Process: a term of 5 (five) years.

2.7.5 As regards the GPS navigation and tracking system used by the Szentkirályi-Kékkúti to track corporate vehicles, three-phase switches to be set according to the nature of the ride, either business, private or field work, have been installed in such vehicles. In the case of private use, the Szentkirályi-Kékkúti allows the Employees to turn off such tracking function, if the corporate vehicle is desired to be used for such private purpose.

3. THE PRECEPTS AND THE METHOD OF THE DATA CONTROLLING PROCESS

3.1 The Data Controller is not entitled to use the defined Personal Data and Information for purposes other than those already defined hereabove.

3.2 In the case of Data Controlling Processes grounded on consent, the Data Subjects are entitled to rescind their consents at any time, which whatsoever will not affect the legality of the Data Controlling Processes having been effective prior to such rescindment.

3.3 Whenever the licit interest of the Data Controller constitutes the legal grounds of the Data Controlling Process, the Data Controller, in full conformity with the provisions set forth in the GDPR, has completed and may complete in the future the so-called "interest assessment test" which will verify that the licit interest of the Data Controller connected with the particular Data Controlling Process outpowers the rights and freedom of the concerned Data Subject connected with the particular Data Controlling Process. In the case of any request in this respect, the Data Controller, according to this Policy, will render written information for the concerned Data Subject regarding the content of this section.

3.4 The Personal Data and Information shall be controlled, managed and handled by the Data Controller in good faith and with respect in full conformity with the principles of transparency, the effective laws and the provisions set forth in this Policy.

3.5 The Data Controller is entitled to control and handle the Personal Data and Information for purposes designated in this Policy and in the concerning laws in effect. The scope of Personal Data and Information is to be proportional to the purpose of the Data Controlling Process, not to be beyond it.

3.6 In each case, whereas the Data Controller desires to use such Personal Data and Information for any purpose other than that of the original data recording, the Data Subjects must be informed of such purpose, for which the preliminary and express consent of the concerned Data Subjects are required, and the Data Controller is liable to ensure the option of refusing such use by Data Subjects.

3.7 The Data Controller will not check the Personal Data and Information provided. Any and all parties providing such Personal Data and Information must solely be responsible for the conformity of any and all such data and information.

3.8 If any Data Controlling Process is to be based on consents, the concerned Personal Data and Information of any and all minors under the age of 16 may be controlled and handled upon the consents of adults in charge of their parental custody. The Data Controller is liable to exert all reasonable efforts to check whether such adults in charge of parental custody have consented to such Data Controlling Process. Any and all measures performed by the Data Controller in this respect, depending on the nature of the Data Controlling Process, are encompassed in the Customized Data Controlling Policies.

3.9 The Data Controller may use the statistically totalized form of the Personal Data and Information, which under no circumstance will contain any data or information expedient to identify and Data Subject, thus it is not qualified as a Data Controlling or Data Forwarding Process.

3.10 The Data Controller is liable to notify any and all concerned Data Subjects of any and all rectifications, restrictions and erasures of any and all Personal Data and Information controlled by it and furthermore to notify all other parties to which such Personal Data and Information were forwarded earlier for the purpose of Data Controlling. Such notification is not required if the licit interest of the concerned Data Subjects is not breached in view of the purpose of the Data Controlling Process.

4. FORWARDING PERSONAL DATA AND INFORMATION

4.1 The Personal Data and Information of any and all concerned Data Subjects are allowed to be disclosed by the Data Controller, if required so by any notification of any official court of law or law enforcement agency or any third party pursuing any legal proceeding in connection with any copyright or property right infringement or any other type of breach or any alleged violation of the law. The disclosure of Personal Data and Information to any third party or any authority, unless stipulated by law otherwise, must be subject to the adjudication/decree of the proceeding authority or to the preliminary and expressed consent of the concerned Data Subject.

4.2 The Data Controller is entitled and liable to forward any and all Personal Data and Information available to and archived legitimately by it to the competent authorities, which data forwarding commitment is required by any law or any arbitration in effect issued by any such authority. The Data Controller will not be responsible for such data forwarding commitment and any consequence arising out of such undertaking.

4.3 If the Data Controller is required to forward the Personal Data and Information, either partly or wholly, to any third party, such Personal Data and Information controlled by it may be forwarded, either partly or wholly, to the concerned third party without the discrete request for the consent

of but upon the preliminary and proper notification to the concerned Data Subject(s) on the condition that such data forwarding commitment will not harm the concerned Data Subject(s) detrimentally according to the provisions set forth in the prevailing content of this Policy. In the case of such data forwarding requirement set forth herein, the Data Controller, prior to such forwarding, is liable to allow the concerned Data Subject(s) to refuse such data forwarding. In the case of any refusal, the forwarding of the Personal Data and Information of the concerned Data Subject(s) described herein is prohibited.

4.4 For the purpose of checking the legality of the data forwarding process and of assuring the information of the concerned Data Subject(s), the Data Controller keeps records of such data forwarding included in APPENDIX 4 [appendix 4] of this Policy.

5. DATA PROCESSORS

5.1 For the purpose of the completion of its operation, the Data Controller engages the services of Data Processors listed in APPENDIX 1 [appendix 1] attached hereto. The discrete consent of any concerned Data Subject is not required for the Data Forwarding Process to any Data Processor listed in this Policy.

5.2 Such Data Processors are not authorized to conclude their own decisions; they are only entitled to proceed as instructed and according to the agreement concluded with the Data Controller. As of May 25, 2018, any and all Personal Data and Information forwarded by the Data Controller to and controlled or processed by the Data Processors must be recorded, controlled and processed by such Data Processors in full conformity with the relevant provisions stipulated by the GDPR.

5.3 The Data Controller is liable to monitor and assess the performance of the Data Processors frequently.

5.4 The consent of the Data Controller is required for the Data Processors to engage the service of any other Data Processor.

6. PARTIES HOLDING ACCESS TO PERSONAL DATA AND INFORMATION

6.1 The Data Controller is liable to ensure that unauthorized parties will not have access to any Personal Data and Information. The restriction of such access is performed by the Data Controller by allowing its Employees to hold the authority of access to files which are necessarily needed for them to perform their jobs/occupations.

6.2 In the case of any unauthorized access, the Data Controller is to conduct an internal investigation to be directed by Dr. Balázs Szabó, Corporate Affairs Director, who will initiate expedient sanctions and/or contemplate the necessity of reporting crime based on the severity of the incident/breach. If the unauthorized access is regarded a Data Breach, the Data Controller will proceed according to Section 8 herebelow.

6.3 The following parties are allowed to hold access to the following types of Personal Data and Information:

TYPES OF PERSONAL DATA AND INFORMATION	PARTIES HOLDING ACCESS TO PERSONAL DATA AND INFORMATION
Personal Data and Information connected with emyployment (applicants, Employees)	HR Director, Corporate Affairs Director, HR Generalist
Personal Data and Information of participants in promotions and events, and of users to Social Media	Staff of the marketing department
Records by the camera surveillance system	Staff of the security department
Records by the GPS navigation system	Staff of the security department
Personal Data and Information of visitors to the Websites	Staff of the IT department and server administrators
Corporate agreements and contracts	Employees in charge of the conclusion and execution of agreements and contracts

7. THE ARCHIVAL AND SECURITY OF PERSONAL DATA AND INFORMATION

7.1 The controlling and archival of the following Personal Data and Information is paper-based:

(a) contracts of employment, lists of attendance, reports of medical checkup by occupational physician, documents of termination of employment from previous job/workplace, documents of termination of employment of employees leaving;

(b) hostess activity information (receipts of presents, information required for mail delivery of prizes in the case of winning players),

7.2 The controlling and archival of the following Personal Data and Information is completed electronically: all other Personal Data and Information not listed in Section 7.1 above, including

(a) Employees' full names, names at birth, mother's maiden names, places and dates of birth, taxation numbers, social security numbers, bank account numbers, permanent and/or temporary addresses/residences, ID Card numbers, reports of medical checkup by occupational physician;

(b) data of Social Media and digital campaigns; sizes of wear and gear;

7.3 As regards the cases listed above, the Personal Data and Information are archived as follows:

(a) Paper-based documents:

The Personal Data and Information are safe deposited in lockable cabinets and/or safes in lockable rooms.

(b) Electronic documents:

The Personal Data and Information are recorded and saved on the hardware of internal servers and on external sites, to which access is granted by restricted security setting and customized eligibility for access to folders and files.

7.4 The Personal Data and Information are secured and safeguarded by several Data and Information Security Measures listed and described in APPENDIX 5 [appendix 5].

8. PROCEDURES TO FOLLOW IN THE CASE OF DATA BREACHES

8.1 If the Data Controller is notified of any Data Breach, it, without unreasonable delay but not later than 72 hours, must notify the Hungarian National Authority for Data Protection and Freedom of Information as well as any and all concerned Data Subjects and must further cooperate fully in order to execute efficient remedial actions as fast as possible under reasonable circumstances.

8.2 The notification must be dispatched electronically marked "URGENT", whose title should read as follows: "URGENT – DATA BREACH" ["SÜRGŐS – SZEMÉLYES ADATOK MEGSÉRTÉSE"].

8.3 Such notification is to include all information regarded relevant in view of the actual Data Breach. The Data Controller's Contact Person must be available for the purpose of prompt assistance and retrospective responses to any query of any Data Subject and of the competent authorities. The template of the notification to be dispatched in the case of any Data Breach is titled Data Breach Report [**Error! Reference source not found.**] in APPENDIX 6 [appendix 6] below.

9. DATA SECURITY OFFICER

Since the Data Controller is neither a public law nor a governmental agency, its scope of main operations is exclusive of specific Data Controlling Processes that require the frequent, systematic and large scale surveillance/monitoring of Data Subjects and such main operations are exclusive of the controlling and handling of the special categories/types of Personal Data and Information OR the controlling and handling of a large amount of data and information regarding criminal actions and adjudications/decrees connected with the assessment of sole criminal responsibilities. Therefore, the Data Controller herein is not obliged by law to appoint any Data Security Officer.

The Data Subjects may make contact with the Contact Person defined in Section **Error! Reference source not found.**5. above in regard to the controlling and handling of their Personal Data and Information.

10. IMPACT ASSESSMENT OF DATA SECURITY

The Data Controller is not obliged to conduct any Impact Assessment of Data Security by virtue of the following reasons:

(a) According to the GDPR, Impact Assessment of Data Security must be implemented in cases, whereas any type of the Data Controlling Process most likely entails high security risks in connection with the rights and freedom of natural persons. Recital 43 of Article 29 Working Party ("**WP29**") includes a list of conditions, the existence of which would most likely imply high risks of the Data Controlling Process. These

conditions encompass systematic surveillance, i.e. Data Controlling Processes completed for the purpose of the surveillance, tracking and control of Data Subjects, which is part of the group of aspects to be considered, because the collection of Personal Data and Information can take place under circumstances, whereas the concerned parties may not be aware of who collects such data and for what purpose. WP29 categorizes the controlling of data and information of Data Subjects, especially of Employees, in exposed situations in the foregoing category.

(b) According to WP29, the more conditions exist in the course of the Data Controlling Process, the more possibility exists that it entails high risks in view of the rights and freedom of the concerned parties/Data Subjects. If less than two conditions exist as to a particular Data Controlling Process, impact assessment is not required as a result of the low level of such risks.

(c) Since the Data Controller properly informs all concerned parties/Data Subjects of all issues related to the camera surveillance system, and since such system is not used for the purpose of monitoring and tracking Employees as exposed parties, the requirement for the completion of an Impact Assessment of Data Security is regarded null and void. As primarily a food manufacturing and marketing business entity, the Data Controller not at all conducts such Data Controlling Processes or applies such technology that would imply relevant risks in view of the rights and freedom of the Data Subjects.

11. EFFACEMENT OF PERSONAL DATA AND INFORMATION

11.1 The Data Controller is to erase, efface and remove any and all Personal Data and Information immediately but within 3 (three) work days at latest

(a) if requested so by any Data Subject or if the consent to the legal grounds of the Data Controlling Process is once rescinded;

(b) if the duration of the Data Controlling Process allowed by law has once ended; OR

(c) if the objective of the Data Controlling Process has once been executed.

11.2 Electronic data to be removed from the server will be deleted.

11.3 Paper-based data to be removed will be annihilated physically by paper shredders.

12. THE DATA SUBJECTS' RIGHTS AND THEIR ENFORCEMENT

The Data Subjects are eligible to exercise their following rights in a written form communicated either electronically or by registered mail addressed to the contacts of the Data Controller listed in Section 1.2.5 above. Such registered mail is considered credible by the Data Controller if the sender Data Subject is unequivocally identifiable on the basis of the application delivered. Any request for information delivered electronically will be considered credible by the Data Controller only if it has been sent from the Data Subject's e-mail address, which on the other hand will not prevent the Data Controller from identifying the concerned Data Subject by any other method.

The Data Controller will immediately evaluate the applications and will make decisions to them that will be delivered to the concerned Data Subject in a written form.

12.1 Right to proper information

12.1.1 The Data Subjects are entitled to request at any time the Data Controller to inform them of whether it controls and handles their Personal Data and Information, and if yes, they are entitled to have and hold access to such data.

12.1.2 Such request for information may be valid to the following: the Personal Data and Information of the Data Subjects controlled by the Data Controller, their sources, the purpose, legal grounds and duration of the Data Controlling Process, the names and addresses of the optionally assigned Data Processors, all activities connected with the Data Controlling Process, which entity has received the Personal Data and information of the Data Subjects and for what purpose if such Personal Data and Information are forwarded.

12.2 Right to rectification

The Data Subjects are entitled to request for the rectification or modification of their Personal Data and Information controlled by the Data Controller. In consideration of the purpose of the Data Controlling Process, the Data Subjects are entitled to request for the amendment to incomplete Personal Data and Information. Subsequent to the satisfaction of any demand for the modification of Personal Data and Information, the previous (erased, effaced) data are no longer allowed to be reconstructed.

12.3 Right to the erasure of the Personal Data and Information

12.3.1 The Data Subjects are entitled to request for the erasure (effacement) of their Personal Data and Information controlled by the Data Controller. Such effacement can be refused (i) for the purpose of exercising the right to the freedom of opinion and expression and to information; OR (ii) if the controlling and handling of Personal Data and information is legitimated by laws; OR (iii) for the purpose of the submission, enforcement and protection of legal claims.

12.3.2 The refusal of the request for erasure will under all circumstances be communicated by the Data Controller to the concerned Data Subject(s), pointing to the reasons of such refusal. Subsequent to the satisfaction of any demand for the modification of Personal Data and Information, the previous (erased, effaced) data are no longer allowed to be reconstructed.

12.4 Right to the restriction of the Data Controlling Processes

12.4.1 The Data Subjects are entitled to request for the restriction of the Data Controlling Processes anent their Personal Data and Information by the Data Controller, if the Data Subjects dispute the accuracy of the Personal Data and Information controlled and handled. In such a case, such restriction is to apply to a particular time period which allows the Data Controllers to check such accuracy. The Data Controller is to mark the Personal

Data and Information controlled and handled by it, if the concerned Data Subject disputes either their accuracy or exactitude, but the inaccuracy or inexactness of the disputed Personal Data or Information is impossible to be concluded unequivocally.

12.4.2 The Data Subjects are entitled to request for the restriction of the Data Controlling Processes anent their Personal Data and Information by the Data Controller, even if such Data Controlling is illegal but the concerned Data Subject refuses the deletion of the Personal Data and Information controlled and requests for the restriction of their use instead.

12.4.3 The Data Subjects are entitled to request for the restriction of the Data Controlling Processes anent their Personal Data and Information by the Data Controller, if the objective of the Data Controlling Process has been attained but the concerned Data Subject requires the Data Controller to keep controlling them for the purpose of the submission, enforcement and protection of legal claims.

12.5 Right to protest

12.5.1 The Data Subjects are entitled to protest the Data Controlling Processes anent their Personal Data and Information (i) if the controlling of their Personal Data and Information is exclusively required for the purpose of executing legal obligations that apply to the Data Controller OR required for the enforcement of the licit interests of the Data Controller or any third party; (ii) if the purpose of the Data Controlling Process is direct business dealing, (market) survey or scientific survey; (iii) the purpose of the Data Controlling Process is the execution of any project of public nature. The Data Controller is to evaluate the legal grounds of the protest of the concerned Data Subject, and if such protest is verified legally grounded, the Data Controlling Process will be finished, the Personal Data and Information subject to such Data Controlling Process will be distrained, and the act of protest and all necessary measures implied will be communicated to all concerned parties to which/whom the Personal Data and Information subject to the protested Data Controlling Process were forwarded earlier.

13. ALTERNATIVES FOR THE ENFORCEMENT OF RIGHTS

13.1 Any query or comment anent the Data Controlling Processes can be delivered to the staff of the Data Controller to the following e-mail address: adatvedelem@szentkiralyi-kekkuti.hu.

13.2 The concerned Data Subjects can communicate their complaints directly to the Hungarian National Authority for Data Protection and Freedom of Information (NAIH); address: H-1125 Budapest, Szilágyi Erzsébet fasor 22/c.; telephone: +36-1-391-1400; e-mail: ugyfelszolgalat@naih.hu; website: www.naih.hu), the contacts of which are as follows:

Address	H-1125 Budapest, Szilágyi Erzsébet fasor 22/c.
Mail address	H-1530 Budapest, Pf. 5
Telephone	+36 1 391 1400

Facsimile	+36 1 391 1410
E-mail	ugyfelszolgalat@naih.hu
Website	www.naih.hu

13.3 If their rights have been violated anyhow, the Data Subjects are entitled to pursue legal remedy. The competent court of law will issue adjudication. Such lawsuit, according to the concerned Data Subject's designation, can be conducted by a court of law whose competent jurisdiction is valid according to the concerned Data Subject's address or residence. Upon request, the Data Controller will inform the concerned Data Subject of the options and means of legal remedy.

14. MODIFICATION OF THIS DATA PROTECTION POLICY

14.1 The Data Controller reserves its right to modify this Data Protection Policy at any time according to its sole, own and unilateral discretion.

14.2 By reading and understanding the modified version of the Data Protection Policy, the Data Subjects accept the prevailing provisions of said Policy in effect, in addition to which the request for the agreement of each Data Subject is not required.

14.3 The date of entering this Policy into effect and its version has been designated on the title page above.

Dated; Budapest, May 25, 2018

Olivér Martin (sgd.)

Managing Director, Country Manager

APPENDIX 1

DATA PROCESSORS

Function	Agency assigned to conduct promotions
Denomination	FastBridge Kft.
Incorporation code	01-09-910619
Business domicile	H-1082 Budapest, Vajdahunyad u. 33–43.
E-mail, telephone no.	office@fastbridge.hu, +36 1 802-5190
Nature of data processing	Processing Theodora consumer promotional registrations and processing data and information connected with Facebook promotions

Function	Agency assigned to conduct promotions
Denomination	Neo Interactive Kft.
Incorporation code	01-09-703098
Business domicile	H-1118 Budapest, Gombocz Zoltán u. 9
E-mail, telephone no.	neo@neo-interactive.hu, +361 789 5000
Nature of data processing	Processing Szentkirályi #egycseppnyar promotional photo uploads and processing data and information connected with Facebook / Instagram promotions

Function	Agency assigned to conduct events
Denomination	Human Telex Kft.
Incorporation code	01-09-064170
Business domicile	H-1036 Budapest, Lajos utca 74-76.
E-mail, telephone no.	hello@humantelex.hu, +36 70 931 38 30
Nature of data processing	Processing consumer contacts at events, settling accounts of presents

Function	Agency assigned to conduct events
Denomination	WONDERDUCK AGENCY Zrt.
Incorporation code	01-10-046174
Business domicile	H-1118 Budapest, Rétköz utca 31. fszt. 1.
E-mail, telephone no.	zoltan.soos@wonderduck.hu, +361 422 3560
Nature of data processing	Processing consumer contacts at events, settling accounts of presents

Function	Agency assigned to conduct partner specific activities
Denomination	Bang Bang Ideas
Incorporation code	13-09-170959
Business domicile	H-2096 Üröm, Tücsök köz 1/c 2. em. 11.
E-mail, telephone no.	brudner.melinda@bangbang.hu; +36 1 610 8952
Nature of data processing	Processing registrations connected with partner specific activities, processing dispatch of presents

Function	Occupational physician
Denomination	Oxygen Medical Újpest
Incorporation code	01-09-911163
Business domicile	H-1042 Budapest, Árpád út 47.
E-mail, telephone no.	info.ujpest@oxygenmedical.hu; +36 1 799 7986

Nature of data processing	Referrals to occupational medical checkups (including Employees' names, occupations, social security numbers, addresses, dates of birth)
Function	Occupational physician
Denomination	Pelso-Med Egészségügyi és Szolgáltató Kft., dr. Ács Károly
Incorporation code	19-09-504596
Business domicile	H-8230 Balatonfüred Csárda utca 1.
E-mail	pelsomed@gmail.com
Nature of data processing	Referrals to occupational medical checkups (including Employees' names, occupations, social security numbers, addresses, dates of birth)
Function	Security operation and maintenance, technical support
Denomination	Hesse Tűz- és Vagyonvédelmi Szolgáltató Kft.
Incorporation code	03-09109512
Business domicile	H-6000 Kecskemét, Tél utca 13
E-mail	biztonsag@hesse.hu
Nature of data processing	Data and information accessed during security operation and maintenance
Denomination	PRINT 2000 Nyomda Kft
Business domicile	H-6000 Kecskemét, Nyomda utca 8.
Incorporation code	03 09 103673
E-mail	soltesz.laszlo@print2000.hu
Nature of data processing	To forward the addresses of sales representatives employed by the Data Controller to Data Processor for the purpose of addressing envelopes
Denomination	ROLL-LAMELL Árnyékolástechnikai Kft.
Business domicile	H-2120 Dunakeszi, Bem József u. 5.
Incorporation code	13 09 115135
E-mail	ocsi@roll-lamell.hu
Nature of data processing	Data and information of the partners of the Data Controller for the purpose of evaluating customized needs for shading
Denomination	H-VILLSZER Kft.
Business domicile	H-1151 Budapest, Székely Elek út 9.
Incorporation code	01 09 700251
E-mail	hvillszer@hvillszer.hu
Nature of data processing	Data and information of the partners of the Data Controller (e.g.: delivery of refrigerators, furniture, etc.), if customized equipment or deliveries are arranged for them

APPENDIX 2

DATA PRIVACY NOTES

PART 1
DATA PRIVACY NOTE FOR APPLICANTS (IN THE SCRIPT OF ADVERTISEMENTS OF VACANCIES)

If you would like to know more about the controlling and processing procedure of your personal data and information specified in the application process for the advertised vacancy, please visit www.szentkiralyi.hu and read our Company's Data Protection Policy.

PART 2
DATA PRIVACY NOTE FOR APPLICANTS REFUSED (REQUEST FOR CONSENT)

We regret to inform you that you have not been selected for an interview for the position advertised. However, if you would like to be informed of similar vacancies at our Company in the future, please confirm your consent by clicking on the icon below. If you desire not to be informed at all, you can unsubscribe at any time.

PART 3
DATA PRIVACY NOTE FOR EMPLOYEES (TO BE CIRCULATED AND UNDERSIGNED AS AN APPENDIX TO BE ATTACHED TO THE CONTRACTS OF EMPLOYMENT)

Adatvédelmi tájékoztató

Ez a dokumentum (a továbbiakban: „Tájékoztató") a Munkavállaló munkaszerződésének melléklete, melyet a Munkavállaló a Szentkirályi-Kékkúti Kft.-vel (székhely: 1117 Budapest, Neumann János u. 1. 1. em.; cégjegyzékszám: Cg.01-09-717667, a továbbiakban: Munkáltató) köt határozatlan időre. A Munkáltatónak a Tájékoztatót elolvasás és megértés után alá kell írnia. A Tájékoztató az Európai Parlament és a Tanács (EU) 2016/679 számú, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló

Data Privacy Note

This document (hereinafter: the "Note") is an addendum to the Employee's employment contract concluded with Szentkirályi-Kékkúti Kft. (registered office: 1117 Budapest, Neumann János u. 1. 1. em.; company registration number: Cg.01-09-717667; hereinafter referred to as the "Employer") for an indefinite term and must be read, understood and signed by the Employee. The Note contains a detailed notification concerning the processing of the Employee's personal data by the Employer in accordance with regulation (EU) 2016/679 of the European Parliament and of the Council on the protection

rendeletének (általános adatvédelmi rendelet, GPDR), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény alapján részletes tájékoztatást tartalmaz a Munkavállaló személyes adatainak Munkáltató által történő kezeléséről az alábbiak szerint:

of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR) and Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as "Information Act") as follows:

1. Cél és jogalap

A Munkáltató a Munkavállaló személyes adatait, munkavállalással kapcsolatos célok érdekében kezeli. Ez magában foglalja az adatok felhasználását a munkaszerződés teljesítésére, a jogszabályi követelményeknek való megfelelésre, és a Munkáltató jogos érdekeinek érvényesítésére. A különböző adattípusok tekintetében az adatkezelési célok és jogalapok részletes listája a Munkáltató Adatvédelmi Szabályzatában található.

1. Purpose and legal basis

The Employer keeps and processes the Employee's personal data for employment purposes. This includes using data to comply with the employment contract, to comply with legal requirements, and pursue its legitimate interests. The detailed list of purposes and legal bases for different data types can be found in the Data Protection Policy of the Employer.

2. Adattípusok

A Munkáltató által kezelt személyes adatok típusai, többek között, magukban foglalják a Munkáltató a http://www.szentkiralyi.hu honlapon hozzáférhető Adatvédelmi Szabályzatának 2.3 pontjában foglalt adatokat, így többek között, a munkavállaló személyi és kapcsolattartási adatait, bérszámfejtéshez, juttatásokhoz és költségekhez szükséges információt, szabadság, betegszabadság és egyéb távollét nyilvántartását; karriertörténettel kapcsolatos dokumentumokat, képzési adatokat, eredményeket, teljesítmény-felméréseket, stb.

2. Types of data

The types of personal data the Employer processes include the data specified in section 2.3 of the Data Protection Policy of the Employer accessible at http://www.szentkiralyi.hu, amongst others, personal identification and contact details of the Employee, information needed for payroll, benefits and expenses purposes; records of holiday, sickness and other absence; and records relating career history, such as training records, appraisals, other performance measures.

3. Egészségügyi adatok

Amennyiben szükséges, a Munkáltató tárolhat a Munkavállalóra vonatkozó egészségügyi adatokat, amelyek magukban foglalhatják a távollét okait, jelentéseket és megjegyzéseket. Ezen adatok kezelésére munkahelyi egészségvédelmi és biztonsági követelményeknek való megfelelés érdekében

3. Health related data

Where necessary, the Employer may keep data relating to the Employee's health, which could include reasons for absence, reports and notes. This data will be used in order to comply with health and safety and occupational health obligations. The Employer will also need this data to administer and manage statutory and

kerül sor. Ezen adatokra ugyanakkor a Munkáltatónak a jogszabályok által előírt és vállalati táppénz, egészségbiztosítás és életbiztosítás adminisztrációja és kezelése miatt is szüksége van.

company sick pay, or health insurance or life insurance policies.

4. Adatok átadása harmadik személyeknek

Az alábbiakban említetteken kívül a Munkáltató csak akkor ad át munkavállalói személyes adatokat harmadik személyeknek, hogyha a Munkáltatót erre jogi kötelezettség terheli, vagy a Munkáltatónak a Munkavállalóval szemben fennálló szerződéses kötelezettségei teljesítéséhez szükséges, például a Munkáltatónak bérszámfejtő, nyugdíj- vagy egészségbiztosító részére kell átadnia azokat.

4. Disclosure to third parties

Other than as mentioned below, the Employer only discloses data of the Employee to third parties if the Employer are legally obliged to do so or where the Employer needs to comply with contractual duties to the Employee, for instance the Employer may need to pass on certain information to an external payroll provider, pension or health insurance schemes.

5. Adatfeldolgozók

A Munkáltató adatfeldolgozóknak munkavállalói személyes adatokat adhat át a munkaviszonyhoz vagy a vállalkozás üzletmenetéhez kapcsolódó célokból, beleértve a bérszámfejtést és egészségügyi vizsgálatot. Az adatfeldolgozók listáját a Munkáltató Adatvédelmi Szabályzata tartalmazza.

5. Data processors

The Employer may transfer data about the Employee to data processors for purposes connected with employment or the management of the company's business including payroll and health check purposes. The list of data processors can be found in the Employer's Data Protection Policy.

6. A személyes adatok tárolása és biztonsága

A Munkavállaló személyes adatai a munkaviszony ideje alatt kerülnek tárolásra, kivéve azokat az adatokat, amelynek megőrzését törvény írja elő, vagy amelyek megőrzéséhez a Munkavállaló hozzájárult. Az adatok megőrzésével kapcsolatos biztonsági intézkedések a Munkáltató Adatvédelmi Szabályzatában találhatóak.

6. Storage and security of personal data

The Employee's personal data is stored for the period of employment except those data whose retention is required by statutory obligation or the Employee provided his consent to holding it. Security measures concerning keeping the data can be found in the Employer's Data Protection Policy.

7. A Munkavállaló jogai

A Munkavállalónak joga van a személyes adataihoz való hozzáféréshez, személyes adatainak helyesbítéséhez vagy azok törléséhez, a személyes adatait érintő adatkezelés korlátozásához, tiltakozhat az adatkezelés ellen.

7. The Employee's rights

The Employee has the right to request access to and rectification or erasure of his personal data, the right to restrict processing, object to processing. The details of such rights can be found in the Employer's Data Protection Policy.

A fenti jogok részletes leírását a Munkáltató Adatvédelmi Szabályzata tartalmazza.

8. Hozzájárulás visszavonása

Abban az esetben, ha a Munkavállaló hozzájárulását adta a személyes adatai kezeléséhez, akkor a Munkavállalónak (bizonyos esetekben) joga van a hozzájárulást bármikor visszavonni, ami azonban nincs kihatással a hozzájárulás visszavonása előtti adatkezelés jogszerűségére.

8. Withdrawal of consent

If the Employee has provided consent for the processing of his personal data, the Employee has the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before the consent was withdrawn.

9. Jogorvoslatok

A Munkavállaónak joga van panasszal fordulni a Nemzeti Adatvédelmi és Információszabadság Hatósághoz vagy a bírósághoz, abban az esetben, ha úgy véli, hogy a Munkavállaló nem felelt meg a Munkavállaló személyes adatainak a kezeléséhez szükséges releváns jogszabályi követelményeknek.

9. Remedies

The Employee has the right to lodge a complaint to the Hungarian Data Protection Office or to the court if he believes that the Employer have not complied with the requirements of the relevant legal rules with regard to the Employee's personal data.

10. Kapcsolattartó

Abban az esetben, ha a Munkavállalónak bármely aggálya támad az adata kezelésével kapcsolatban, a Munkavállaló az alábbi személyt keresheti felvilágosítás végett: [név], személyesen vagy e-mail ([email cím]) útján.

10. Contact person

If the Employee has any concerns as to how his data is processed, the Employee can contact [név] either personally or via e-mail ([email cím]).

11. Adatvédelmi Szabályzat

További információt a Munkavállaló a Munkáltató honlapján feltüntetett Adatvédelmi Szabályzatban találhat.

11. Data Protection Policy

For further information, the Employee can consult with the Employer's Data Protection Policy which can be accessed at the Employer's website.

PART 4
DATA PRIVACY NOTE INCLUDED IN CONTRACTS CONCLUDED WITH SUPPLIERS/VENDORS

The Personal Data and Information of the Contact Person designated in this Contract may be controlled and processed by the Szentkirályi-Kékkúti Kft. for the purpose of fostering its licit interests. The relevant specifications regarding the controlling and processing procedure of any and all Personal Data and

Information have been defined in the Data Protection Policy of the Szentkirályi-Kékkúti Kft. available on its website: www.szentkiralyi.hu.

PART 5
CONSENT TO THE DELIVERY AND ACCEPTANCE OF PROMOTIONAL PRESENTS

By clicking on the following [link] / [signature], you will consent to the controlling and processing of your personal data and information ([*data and information to be controlled and processed to be listed herein*]) by the Szentkirályi-Kékkúti Kft. to the extent required. The relevant specifications regarding the controlling and processing procedure as well as your rights and eligibilities have been defined in the Data Protection Policy of the Szentkirályi-Kékkúti Kft. available on its website: www.szentkiralyi.hu.

PART 6
DATA CONTROLLING NOTES CONNECTED WITH PERSONAL DATA AND INFORMATION CONTROLLED AND PROCESSED IN THE COURSE OF DIRECT MARKETING COMMUNICATED TO CONSUMERS

Newsletters and Direct Marketing:

If you would like to receive newsletters regarding events, news and promotional campaigns of the Szentkirályi-Kékkúti Kft, please click on the following icon. By clicking on the icon, you will consent to the controlling and processing of your personal data and information ([*data and information to be controlled and processed to be listed herein*]) by the Szentkirályi-Kékkúti Kft. in full conformity with its Data Protection Policy which is available on its website [www.szentkiralyi.hu]. If you desire not to receive any newsletter at all in the future, please click on the "Unsubscribe" icon in the lowest part of the newsletters in order to unsubscribe at any time.

Events:

This is to inform you that your personal data and information ([*data and information to be controlled and processed to be listed herein*]) will be controlled and processed in connection with your participation in the event. The relevant specifications regarding the controlling and processing procedure as well as your rights and eligibilities have been defined in the Data Protection Policy of the Szentkirályi-Kékkúti Kft. available on its website [www.szentkiralyi.hu].

Raffles and Sweepstakes:

By taking part in the raffles and sweepstakes, you will consent to the controlling and processing of your personal data and information ([*data and information to be controlled and processed to be listed herein*]) by the Szentkirályi-Kékkúti Kft. required for the purpose of your participation to the extent necessary for their availability. The relevant specifications regarding the controlling and processing procedure as well as your rights and eligibilities have been defined [*title of the customized informational document of the raffles and sweepstakes to be inserted*]: [*link of the customized informational document of the*

raffles and sweepstakes to be inserted] and in the Data Protection Policy of the Szentkirályi-Kékkúti Kft. available on its website [http://www.szentkiralyi.hu].

Add-ons/Extensions on Social Media pages:

This is to inform you that your personal data and information will be controlled and processed in connection with your actions on the page. The relevant specifications regarding the controlling and processing procedure have been defined in the Data Protection Policy of the Szentkirályi-Kékkúti Kft. available on its website [http://www.szentkiralyi.hu].

PART 7
NOTE OF THE USE OF COOKIES ON THE WEBSITES

"Cookies" are a collection of information transferred to the users' computers that visit the Websites. Cookies help run the Websites, contribute to their more efficient operation and communicate information to the owners of the Websites.

Cookies are used by Szentkirályi-Kékkúti to improve the usability and functionality of the Websites and to have a better understanding of how the Websites, and the tools and services displayed on them are used by the visitors. Cookies are stored on the computers of visitors that visit the Websites in order to provide more entertaining and enjoyable Websites with them the next time they visit these Websites. Such information, based on which surveys can be carried out regarding the visitors' demographical data and scopes of interests, are used solely internally (within the KMV Corporate Group). Anonymous data and information of generic nature that will NOT lead to the identification of persons visiting the Websites are NOT defined as personal data and information in the GDPR and the Infotv.

Szentkirályi-Kékkúti never uses Cookies for the purpose of collecting data and information, such as names, suitable for the identification of persons but reserves its right to connect information contained in the Cookies with personal data and information obtained by other means from the visitors of the Websites.

The settings of Cookies can be reset at any time in the browsers of visitors visiting the Websites. Importantly, if such settings have once been reset, NOT all functions of the Websites may be used.

The following types of Cookies are used when the Websites are visited:

(a) Cookies required for the operation of the Websites;

These Cookies are required by all means for the operation of the Websites. Without these, the Websites will not run properly.

(b) Cookies assisting the operation of the Websites

These Cookies assist in operating the Websites for a better quality. For instance, specific Cookies remember contents viewed on the Websites earlier. Cookies assisting in operating

the Websites therefore allow the use of contents in a customized manner that suits the interests of the visitors and save time by avoiding requesting for information already given earlier, when the users revisit the Websites or attempt to enter parts that require registration.

(c) First Party Cookies

These Cookies are directed by this Website and are solely read by this Website

(d) Third Party Cookies

These Cookies are directed by third parties and are used for different services.

(e) "Flash" Cookies

Apart from the above, Szentkirályi-Kékkúti uses "flash" cookies as well. The purpose of these flash cookies is to control and handle the settings of the visitors (e.g.: volume setting, the highest scores in a game, etc.) that visit the Websites for the purpose of setting the contents properly. Third parties that are partners to Szentkirályi-Kékkúti and render particular services (e.g.: games, advertisements) use these flash cookies for purposes other than the collection of data and information of personal identification nature

PART 8
INFORMATION REGARDING MONITORING AND SURVEILLANCE BY GLOBAL POSITIONING SYSTEM (GPS)

The locations and routes of the company vehicle you are authorized to use are monitored by a GPS tracking and navigation system of the Szentkirályi-Kékkúti Kft. The purpose of such surveillance is as follows: [*e.g.: accurate planning of particular work processes, tracking the route of a cargo or vehicle of high value, safeguarding an Employee's' life or physical condition, checking the location of an Employee that drives en route to a destination defined, stb.*]. Data and information recorded by the GPS System will be archived and preserved for a term of [*duration*]. For further information, please read the Data Protection Policy of the Szentkirályi Kékkúti Kft. available on its website [www.szentkiralyi.hu] or make contact with [*e-mail address of the contact person in charge of matters connected with data protection*].

PART 9
INFORMATION REGARDING CAMERA SURVEILLANCE

[camera icon]

This area is under camera surveillance. The purpose of surveillance: [e.g.*: personal security, protection of equipment of high value, etc.*] The camera surveillance system is operated by the Szentkirályi-Kékkúti

Kft. Images, visuals, events and incidents will be archived and preserved for a term of [3 (three) work days] / [30 (thirty) work days]. The checkpoint in charge of camera surveillance will allow access to the Camera Surveillance Policy as well as to the specific descriptions and maps of the positions of the cameras, the sectors within their viewing angles, and the purposes of their operation. For further information, please read the Data Protection Policy of the Szentkirályi Kékkúti Kft. available on its website [www.szentkiralyi.hu].

APPENDIX 3

SPECIFIC DIRECTIONS OF THE OPERATION OF THE SECURITY CAMERA SURVEILLANCE SYSTEM

1. Composed of 72 cameras, a closed-circuit television and camera surveillance system (hereinafter referred to as "**CamSystem**") has been installed to operate on the sites of Szentkirályi-Kékkúti for the purpose of the protection of the physical condition of the Empoyees of Szentkirályi-Kékkúti and of other parties and persons visiting such sites and for the purpose of securing the property and assets on such sites of Szentkirályi-Kékkúti. In the course of its operation, the visuals and images (hereinafter referred to as "**Visual Records**") of the Employees of Szentkirályi-Kékkúti and of other parties and persons visiting the sites of Szentkirályi-Kékkúti are recorded, which Visual Records are qualified as Personal Data.

2. The CamSystem, which is equipped with a tracking system, digitally records the Visual Records. The CamSystem records all motions, days, dates/times and places confined within the site subject to camera surveillance. The cameras operate for 24 (twenty-four) hours 7 (seven) days a week. Depending on the positions of the cameras, the quality of the Visual Records allows the identification of natural persons. The positions of the majority of the cameras are fixed, while some of them have optical zoom functions in order to allow the tracking of a particular person or place closely, just in case. The CamSystem does not use any intelligent technology, neither is it connected to any other system and is unable to record voices, sounds or noises. No camera has been installed in particular sectors (e.g.: locker rooms, toilets, etc.), whereas the privacy of the Data Subjects must be respected definitely.

3. The Personal Data recorded on the Visual Records have been controlled and processed by the Data Controller for the enforcement of its licit business interests in full conformity with the purposes set forth in Section 5 below (Art. 6 (1) (f) of GDPR).

4. The Personal Data recorded on the Visual Records may be used until the expiry of the duration designated in Section 5 below, except if the Personal Data and Information are to be used as exhibits in the course of any court proceeding or of any investigation by any authority in full conformity with Article (5) of Par. 31 of the Personal and Property Security Act,

5. Upon request, the checkpoints of the sectors under CamSystem surveillance will allow access to the specific descriptions and maps of the positions of the cameras, the sectors within their viewing angles, and the purposes of their operation.

   The Visual Records can be accessed by *Security Officer György Varga* and, in his absence, by *Security Guard on Duty Zsolt Lingurár* as Employees of the Szentkirályi-Kékkúti and, if any technical support (e.g.: CamSystem operation maintenance) is necessary, by the Data Processor defined in Section 7 below that must adhere to the instructions of Szentkirályi-Kékkúti under its supervision under all circumstances. Any third party that is to control and/or process the Personal Data recorded on the Visual Records OR that which, for any reason, is eligible to have access to such data is liable to record its denomination, the reason for and time/date of access to such data in minutes.

6. According to a written agreement concluded with Szentkirályi-Kékkúti, Hesse Biztonságtechnika (business domicile: H-6000 Kecskemét, Tél utca 13.; incorporation code: 03-09109512) as Data Processor has been responsible for the performance of any and all assignments of technical support (e.g.: CamSystem operation and maintenance) as to the CamSystem.

7. As regards the Data Controlling Process of the Personal Data and Information recorded by the CamSystem, the Data Subjects are entitled to reserve their rights and rights to legal remedy set forth in Sections 13 to 14 of this Policy, on the condition that such rights of any and all Data Subjects can be restricted if such restriction is required for the protection of the rights and/or freedom of the concerned Data Subjects and/or of other concerned parties (e.g.: any Data Subject that desires to gain access to Visual Records which display any third party whose consent has not been obtained, assuming that the CamSystem does not allow to render the Visual Records of other parties unrecognizable).

APPENDIX 4

DATA FORWARDING FILE

APPENDIX 5

DATA AND INFORMATION SECURITY MEASURES

1. ACCESS CONTROL:

The Data Controller is to prevent any unauthorized person or party from acquiring access to systems ("**Data Controlling Systems**") by which the Personal Data and Information are processed. In order to do so, at least the following actions are to be taken:

Access Control System (ID card reader, integrated circuit card, chip card)
Door Locking System (electronically locked doors, etc.)
Security Service, security guards
Monitoring and Surveillance System (alarm system, video/CCTV monitors)

2. ENTRY CONTROL:

The Data Controller is to prevent any unauthorized person or party from using and/or acquiring access to the Data Controlling Systems. In order to do so, at least the following actions are to be taken:

Passwords (special characters, minimum length and password change)
Automatic lock-out (e.g.: wrong password, time-out)
Encryption of data carriers

3. ELIGIBILITY FOR ACCESS CONTROL:

The Data Controller is to guarantee that any and all parties that use the Data Controlling Systems via which they can gain access to Personal Data and Information will have a special eligibility for access as to such data and information which are not allowed to be read, copied, modified or deleted without authorization. In order to do so, at least the following actions are to be taken:

Special eligibility for access (profiles, roles, transactions and processes)
Controlling eligibility for access
Tracking the modifications of the eligibilities for access
Erasure of the eligibilities for access
In the case of the termination of the effect of any Employee's employment, the effacement/rescindment of the eligibilities for access is a proper process that needs to include the following:

(f) the rescindment of all eligibilities for access to the system;
(g) disabling the user' account and the deletion of mobile applications used for processing Personal Data and Information;
(h) repossession of IT tools (e.g.: laptop) used for processing Personal Data and Information;
(i) rescindment of the eligibility for physical access to site;
(j) repossession and annihilation of the ID card for access.

4. USERS CONTROL:

The Data Controller is to eliminate the unauthorized use of the automated Data Controlling Systems. In order to do so, at least the following actions are to be taken:

Contracts/agreements of binding nature to be concluded with users, which contain, amongst many, obligations and responsibilities regarding the adherence to the secrecy, informatics and security policies

Password use (including special characters, minimum length and password change each period of 90 days)

5. DATA FORWARDING CONTROL:

The Data Controller is to guarantee that, in the course of the electronic data forwarding processes, the Personal Data and Information are impossible to be read, copied, modified or removed illicitly, or that the same misacts are impossible to be done in the process of copying, archival or forwarding on data carriers. In order to do so, at least the following actions are to be taken:

Encryption
VPN

6. DATA ARCHIVAL AND STORAGE CONTROL:

The Data Controller is to prevent unauthorized third parties from accessing to Personal Data and Information and from illicitly accessing to, modifying or erasing such data and information archived and/or stored (data archival/storage control). In order to do so, at least the following actions are to be taken:

Data archival/storage control

7. DOCUMENTATION CONTROL:

The Data Controller is to guarantee that it is capable of controlling and monitoring the documentation of all relevant processing phases of the Data Controlling Systems and of tracking particular phases of the Personal Data and Information processing procedure. In order to do so, at least the following actions are to be taken:

Documentation of the processing activities

8. DATA RECOVERY CONTROL:

The Data Controller is to maintain the data recovery function of the installed Data Controlling Systems to be prepared for any technical error. In order to do so, at least the following actions are to be taken:

Data saving (frequent backup saving; no data of private nature are allowed to be saved on the servers)

Remote Storage

Disaster Recovery Plan (DRP)

9. AVAILABILITY CONTROL:

The Data Controller is to avoid the contingent obliteration and/or loss of Personal Data and Information, hence to maintain their uninterrupted availability for the Data Controller (availability control). In order to do so, at least the following actions are to be taken:

Data saving processes/security data saving
Data storage virtualization technology (e.g.: RAID technology)
Uninterrupted Power Supply
Remote Storage
Antivirus apps/firewalls
Disaster Recovery Plan (DPR)

APPENDIX 6

DATA BREACH REPORT

ADATVÉDELMI INCIDENS BEJELENTÉSE [MINTA]
SÜRGŐS!

CÍMZETT:
KÜLDŐ:

Cégnév:

Küldő személy neve: []
- **e-mail címe:** []
- **telefonszáma:** []
- fax-száma: []
- egyéb: []

KÜLDÉS DÁTUMA ÉS IDEJE: [Adatkezelő]

KÜLDÉS MÓDJA:
- e-mailen
- faxon
- egyéb: []

1. KAPCSOLATTARTÓI ADATOK

1.1 Az Adatkezelő neve és címe:

1.2 Az Adatkezelő kapcsolattartójának neve:

1.3 Az előbbi személy elérhetőségei (telefonszám, mobiltelefonszám, email-cím):

2. A SZEMÉLYES ADATOK MEGSÉRTÉSE VONATKOZÓ LEGFONTOSABB ADATOK ("ELSŐ RÉSZ")

2.1 Az Adatvédelmi Incidens bekövetkeztének időpontja, szükség esetén becslés alapján:

2.2 Az Adatvédelmi Incidens észlelésének időpontja:

2.3 A Személyes Adatok megsértésének módja és körülményei:

DATA BREACH REPORT
[SAMPLE]
URGENT!

TO:
FROM:

Name of company:

Sender's name: []
- **email address: []**
- **telephone: []**
- fax: []
- other: []

SENDING DATE: [Adatkezelő]

FORM OF SENDING:
- via email
- via fax
- other: []

1. DATA OF CONTACT PERSON

1.1 Name and address of the Data Controller:

1.2 Name contact person at the Data Controller:

1.3 Contact information of the person above (phone number, mobile, email address):

2. THE MOST IMPORTANT DATA CONCERNING THE PERSONAL DATA BREACH ('FIRST PART')

2.1 Date of the occurrence of the Data Breach (based on estimation, if necessary):

2.2 Date of the detection of the Data Breach:

2.3 Form and circumstances of the Personal Data Breach:

2.4 Az érintett Személyes Adatok jellege és tartalma:

2.5 Az Adatkezelő által az érintett személyes adatok védelmére alkalmazott vagy alkalmazni tervezett műszaki és szervezeti intézkedések:*

3. A SZEMÉLYES ADATOK MEGSÉRTÉSE VONATKOZÓ TOVÁBBI ADATOK ("MÁSODIK RÉSZ")

3.1 Az Adatvédelmi Incidens összefoglalása, megjelölve az adatok megsértésének fizikai helyét és az érintett adathordozót is:

3.2 Az Érintettek száma:

3.3 A lehetséges következmények és kedvezőtlen hatások ismertetése az Érintettekre nézve**:

3.4 A lehetséges kedvezőtlen hatások enyhítésére az Adatkezelő által alkalmazott műszaki és szervezeti intézkedések:

4. HATÁRON ÁTNYÚLÓ VONATKOZÁSOK (HA VANNAK)

4.1 Az Érintettek között vannak-e más EU tagállamokban élő érintettek:

2.4 Type and content of the Personal Data in question:

2.5 Technical and organisational measures used or planned by the Data Controller to protect the Personal Data in question:*

3. ADDITIONAL INFORMATION REGARDING THE PERSONAL DATA BREACH ('SECOND PART')

3.1 Summary of the Data Breach, marking the physical place and the medium of the Data Breach:

3.2 Number of Data Subjects involved:

3.3 Description of possible consequences and unfavourable effects for Data Subjects**:

3.4 Technical and organisational measures used by the Data Controller to mitigate the possible unfavourable consequences:

4. CROSS-BORDER RELATED ISSUES (IF ANY)

4.1 Any of the Data Subjects living in other EU member states:

Megjegyzések az űrlap kitöltéséhez:

*** Megjegyzés a fenti 2.5 ponthoz**
Rendkívül fontos részletes tájékoztatást nyújtani azzal kapcsolatban, hogy a *megfelelő technikai védelmi intézkedéseket végrehajtották-e*, vagy, hogy *ezen intézkedéseket alkalmazták-e a biztonság sérelmével érintett adatok tekintetében*.

**** Megjegyzés a fenti 3.3 ponthoz**
Lényeges körülmény, hogy az Adatvédelmi Incidens, azaz a személyes adatok megsértése várhatóan hátrányosan érinti-e az Érintettek személyes adatait vagy magánéletét. A tekintetben, hogy az Adatvédelmi Incidens várhatóan hátrányosan érinti-e az Érintettek személyes adatainak vagy magánéletének védelmét, különösen az alábbiakat kell figyelembe venni:

a) az érintett személyes adatok jellegét és tartalmát, különösen akkor, ha azok *pénzügyi információkat*, *különleges adatokat* (pl. vallási, etnikai, szexuális irányultságra vonatkozó, egészségügyi és hasonló adatok), *helymeghatározási adatokat*, *internetes naplófájlokat*, *internetes böngészési*

Notes for filling the form:

*** Note for point 2.5 above**
It is highly important to provide detailed notification regarding *whether the appropriate technical protection measures have been implemented* or *whether those measures have been applied to the data affected by the Data Security Breach.*

**** Note for point 3.3 above**
It is an important circumstance whether the Data Breach, i.e. the breach of personal data is likely to adversely affect the Data Subjects' personal data or private lives. In regards whether the Data Breach would adversely affect the Data Subjects' personal data or private lives, the following shall be considered in particular:

a) type and content of the affected personal data, especially if they affect *financial information, sensitive data* (e.g. concerning religious, ethnical, sexual orientation, medical and similar data), *localisation data, internet log files, internet browsing history, electronic mailing data;*

előzményeket, *elektronikus levelezési adatokat* érintenek;

b) a személyes adatok megsértésének várható következményeit az Érintettre nézve, különösen akkor, ha a személyes adatok megsértése személyes adattal visszaéléshez, testi épség sérelméhez, becsületsértéshez, rágalmazáshoz vagy a jóhírnév sérelméhez vezethet; valamint

c) a személyes adatok megsértésének körülményeit, különösen akkor, ha a Büntető Törvénykönyvről szóló 2012. évi C. törvényben szabályozott *tiltott adatszerzés* vagy *információs rendszer vagy adat megsértése*, valamint az *információs rendszer védelmét biztosító technikai intézkedés kijátszása* bűncselekmények gyanúja merül fel, vagy az Adatkezelő tudomással bír arról, hogy az adatokat az adatkezelésre nem jogosult személyek kezelik.

b) the expected consequences of the personal data breach regarding the Data Subject, especially if the breach of the personal data could result personal data abuse, violation of physical safety, slander, defamation or damage to reputation; and

c) the circumstances of the breach of personal data, especially if there is a suspicion of the crimes of *illicit access to data, breach of information system or data, or compromising or defrauding the integrity of the computer protection system or device* regulated in Act C of 2012 on the Criminal Code, or the Data Controller has the knowledge that the data is controlled by persons who do not have the right to control the data.