OUR DATA MANAGEMENT PRINCIPLES

GENERAL DATA PROTECTION AND DATA SECURITY POLICY

(STUDIO IN-EX PLC)

Valid from 25.05.2018

I. GENERAL PROVISIONS

DETAILS OF THE COMPANY

- Company name: STUDIO IN-EX PLC (hereinafter referred to as the Company)
- Company registration number: 01-10-049782
- Registered office: 1097 Budapest, Könyves Kálmán krt 11. building A. 1st floor
- Tax number: 26321512-2-43
- Legal representative: Molnár Balázs CEO
- For data protection complaints, please contact the HR Coordinator

1. Purpose and scope of the regulation

The purpose of the regulation is to

(i) define the procedures for the processing of personal data held by the Company, whether in manual or computerised form records kept by the Company,

(ii) ensure compliance with the constitutional and civil law principles of data protection and the requirements of data security;

(iii) prevent unauthorised access to personal data, alteration of data, unauthorised disclosure of personal data, unauthorised disclosure of personal data to third parties, prevent the unauthorised disclosure or any other breach; and

(iv) regulate the Company's internal data management procedures on the basis of the above.

The scope of the regulation covers all activities of all employees and subcontractors of the Company - and manual processing of personal data by all employees and contractors of the Company.

The personal scope of the regulation extends to all employees of the Company performing data management and data processing, as well as natural and legal persons having a contractual relationship with the Company, legal persons having legal personality, and legal entity, to the extent specified in the contract or confidentiality agreement concluded with them.

The subcontractors and persons covered by the scope of application and the scope of personnel are deemed to accept this regulation.

2. Applicable laws and internal regulatory documents

From the point of view of data management, the following applicable laws are relevant, which may change from time to time. In the event of a change in legislation, the change required by the current legislation must be considered for a given part of the regulations, and the data controller will take the necessary measures to amend the regulation as soon as possible.

More important relevant legislation:

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 and repealing Directive 95/46/EC (General Data Protection Regulation)

• Act V of 2013 on the Civil Code (hereinafter: "Civil Code"),

• Act I of 2012 on the Labor Code (hereinafter: "Mt."),

• Act CXII of 2011 on informational self-determination and freedom of information (hereinafter: "Infotv."),

• Act C of 2000 on Accounting

Related internal regulatory documents:

• Document Management Regulation

• Regulation on IT security

3. Concept definitions

If there is a discrepancy between the terms below and the legal term, the legal definition shall be accepted.

Data:

The appearance form of information, i.e. the uninterpreted but interpretable form of communication of facts and ideas.

Information:

Information is data interpreted as new knowledge, which can be sensed, detected and perceived.

Information self-determination right:

The right to informational self-determination is a basic citizen's right guaranteeing the protection of personal data. Subject is personal data.

Employment register:

The register containing data created in connection with the employment relationship and related to it.

Personal document:

All data carriers – created on any material, form and using any device – that are created when, during or after the employment relationship is established and contain data and information related to the employee.

Data protection:

Legal processing of personal data by the persons concerned set of principles, rules, procedures, data management tools and methods ensuring its protection.

Data management:

Regardless of the process used, any operation performed on the data, such as collection, recording, organisation, storage, alteration, use, retrieval, disclosure, transmission, alignment or combination, blocking, erasure and destruction of data, prevention of their further use, taking of photographs, audio or video recordings, and recording physical characteristics and any other form of personal identification of a data subject (fingerprints or palm prints, DNA sample, iris scans, etc.) which may be used to identify the person.

Data Controller:

The person or organisation that determines the purposes for which the data are processed, takes and implements decisions concerning data management (including the tool used), or has them implemented by the data processor they have commissioned.

Data processing:

Carrying out technical tasks related to data management operations (regardless of the method and tool used to perform the operations, as well as the place of application).

Data processor:

The person or organisation that processes data on the basis of a contract with the controller - including a contract based on the provisions of the law – processes the data. The General Data Protection Regulation of the European Union contains a different definition!

Rights of the person concerned:

The data subject must be clearly informed of all the details of the data management even before the data management starts, but also at any time upon request. The data subject may also request the rectification or, in certain cases, the erasure of his or her data, and may object to the processing of his or her personal data in cases defined by law.

Principles of data management:

The requirement of purpose-bound data management (see below) as well as the requirement of data quality. The latter includes the need for accurate, complete and up-to-date data, as well as the fair and legal nature of data collection and data management.

Data management for specific purposes:

Personal data may only be processed for a specific purpose, in order to exercise rights and fulfil obligations. In all stages of data management, the purpose of data management must be met, the collection and management of data must be fair and legal. Only personal data that is essential for the realization of the purpose of data management and suitable for achieving the purpose can be processed. Personal data can only be processed to the extent and for the time necessary to achieve the purpose. During data management, it must be ensured that the data are accurate, complete and - if necessary in view of the purpose of the data management - up-to-date, and that the data subject can only be identified for the time necessary for the purpose of the data management.

Job applicant:

A person who registers his/her personal data on the DATA CONTROLLER's website in the DATA CONTROLLER's database (whether for specific job offers or not).

Client:

The legal or natural person who uses a service of the DATA CONTROLLER.

Prospective client:

The legal or natural person who is expected to use a service of the DATA CONTROLLER.

3. Possible differences between individual policies and regulations

The Company is a data controller for some of the services described below and a data processor for some services. Data processing activities are governed by the provisions of the contract concluded with the data controller and its annexes. In the event of any deviation, the legal provisions always govern, except in cases where the law allows a deviation. In these cases, this General Data Protection and Data Security Regulation as well as the contract with the data controller shall govern.

4. Principles of data management and data processing

Personal data may only be processed for specific purposes, in order to exercise rights and fulfil obligations. At all stages of data management, the purpose of data management must be fulfilled and the collection and management of data must be fair and legal. Only personal data that is necessary for the purpose of the data management and is suitable for the purpose shall be processed. Personal data may only be processed to the extent and for the duration necessary to achieve the purpose (unless it is the purpose) in accordance with the provisions of this regulation.

Before data processing begins, the person concerned must be informed clearly and in detail about all the facts related to the processing of his/her data, in particular the purpose and legal basis of data processing, about the data management and data processing, the duration of data processing, if the data subject's personal data is processed by the Company as data controller pursuant to the basis of § 6, paragraph (5)of the Privacy Act and about who can see the data. The information must also cover the data subject's rights and legal remedies.

Accountability: The controller is responsible for compliance with the following principles and must be able to demonstrate this compliance. If the Company performs a data processing task, it helps the fulfilment of the basic principles and its accountability to the maximum extent.

(1) Legality, fair procedure and transparency

The Company shall process personal data in a legal and fair manner that is transparent to the data subject.

(2) Purpose limitation

Data shall be collected only for specific, explicit and legitimate purposes and they should not be handled in a way that is incompatible with these purposes; in accordance with Article 89(1), further data processing for the purpose of archiving in the public interest, for scientific and historical research purposes, or for statistical purposes is not considered incompatible with the original purpose.

(3) Data saving

The principles must be appropriate and relevant for the purposes of data management and must be limited to what is necessary.

(4) Accuracy

Data must be accurate and, where necessary, up to date; all reasonable measures must be taken to ensure that personal data which are inaccurate for the purposes of data management are promptly deleted or corrected without undue delay.

(5) Limited storage capacity

It must be stored in a form that allows the identification of the person concerned only for the time necessary to achieve the goals of personal data management; personal data may be stored for a longer period only if the personal data will be processed in accordance with Article 89(1) for the purpose of archiving in the public interest, for scientific and historical research purposes or for statistical purposes, the rights of the person concerned taking into account the implementation of the appropriate technical and organizational measures required to protect his freedoms.

(6) Integrity and confidentiality

Data shall be processed in such a way that adequate security of personal data is ensured by the application of appropriate technical or organizational measures, including protection against unauthorised or illegal processing, accidental loss, destruction or damage of the data.

5.Lawfulness of data management

As of May 25 2018, the processing of personal data is only legal if and to the extent that at least one of the following is met:

a) the person concerned has given appropriate, informed and voluntary consent to the processing of his personal data for one or more specific purposes;

b) data processing is necessary for the performance of a contract in which the person concerned is one of the parties, or it is necessary for taking steps at the request of the person concerned prior to the conclusion of the contract;

c) data management is necessary to fulfil the legal obligation of the data controller;

d) data processing is necessary to protect the vital interests of the person concerned or another natural person;

e) data processing is in the public interest or is necessary for the execution of a task performed in the context of the exercise of public authority delegated to the data controller;

f) data management is necessary to enforce the legitimate interests of the data controller or a third party, unless the interests or fundamental rights and freedoms of the person concerned take precedence over these interests, which require the protection of personal data, especially if the person concerned is a child.

The legal basis for each of the company's data processing is summarized in the table below:

Managed personal data	Categories of data	Legal basis
Website visitors	Information stored in cookies	Contribution
Job applicants	Contact details, biographical data	Contribution
Representatives and employees of business partners	Contact details	Consideration of interests based on legitimate interests Legitimate interest: for the continuity of the Company's business vested interest
Data of registrants to the career portal	See on the career portal	Contribution
Newsletters, referrals, e-mail address	Interest, qualifications / data related to education	Contribution
Headhunting services	Autobiographical data, tests and their results, data recorded during an interview	Consent, or if we use data made public on public social networking portals (e.g. linkedin.com) for networking purposes, consideration of interests based on the client's legitimate interests. Legitimate interest: finding a quality workforce, based on public data

6. Data processing

The Company, as data controller uses data processors: employees, subcontractors, all of whom have accepted this regulation and are bound by confidentiality. If the Company performs recruitment services at the request of its clients, the Company is a data processor (and in the case of registered jobseekers, a Data Controller).

7. Data transfers

During the recruitment service, the Company forwards the data of job applicants to its clients and partners. Transfers are made to specific information may be requested.

8. Right of legal redress

The Company's managers are obliged to continuously monitor compliance with the legal requirements and internal regulatory documents related to data protection. The internal data protection officer / data protection officer is entitled to verify that the data management is legal by reviewing the internal regulatory documents, protocols and records related to document and data management maintaining order. In the case of a breach of the law, it calls on the person managing the data or the head of the organizational unit to terminate it, and in the case of a particularly serious breach of the law, it turns to the CEO. The internal data protection officer is authorised to check the system of personal and employment records.

Supervisory authority:

National Authority for Data Protection and Freedom of Information

1125 Budapest, Szilágyi Erzsébet fasor 22/C

If you wish to seek judicial remedy: The Courts have jurisdiction, with the fact that the court of the place of residence of the person concerned shall also have jurisdiction.

II. DETAILED RULES

1. Data protection register

The Company shall, through the Data Protection Officer, keeps a record of all data processing carried out in the Company or on behalf or for the account of the Company, documenting the main facts and circumstances related to data processing. ....., as a data processor, provides the cloud-based recruitment system (.....) on which the data is stored and from which it is transmitted and where the various records are generated. The Company is convinced that the ..... Information Security and Data Processing provisions comply with the aspects prescribed by law.

2. Transmission of personal data

In the context of a contract to be concluded with a person or organization carrying out data management or data processing on behalf of and in the interest of the Company, the Company is obliged to ensure that data protection requirements and guarantees are included in the text of the contract.

The Company's Client may store the Job Applicants' materials until the goal is reached, in accordance with the relevant legislation at the time, and in particular the CXII of 2011 on the right to informational self-determination and the freedom of information law and Regulation (EU) 2016/679 of the European Parliament and of the Council (EU) of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). The data will be treated confidentially and lawfully and will be used only for the purpose of filling a specific vacancy in relation to the specific open position already granted at the time of use and will not be disclosed or made available to third parties after the position has been filled.

Both the Company and the Company's client undertake and guarantee that they will cooperate fully and in all respects with regard to the fulfilment of the requests made by the applicants, answering the requests, and any possible official and/or court proceedings.

3. Notification of complaints / claim

Filing a claim to the Company:

The Company may provide you with several ways to report specific claims related to each of its Services: in writing, by email. If you give the Company the opportunity to submit a claim via email, the claim received from the e-mail address previously provided to the Company in connection with the Service - and only from this e-mail address – shall be deemed to be a claim received from the person concerned. In the case of requests submitted from another email address, as well as in writing, it is mandatory to confirm the request from the email address provided at the time of registration, or to change the registration email address accordingly.

If the Company's data management is not based on the persons concerned consent, but the data management was initiated abusively by a third party, the person concerned may request the erasure of personal data published about him which have been disclosed by another person, and information on the processing, subject to appropriate proof of his/her identity and his/her connection with the personal data.

In the event of the death of the person concerned, any close relative of the person concerned or of a person to whom he or she has received a testamentary benefit may, by presenting the death certificate or by sending a copy to the Service's customer service address, request the erasure of data relating to a job applicant or a client or prospective client, and the transfer of the data, subject to proof of his or her legitimate interest, and upon proof of his or her relationship with the person concerned.

The DATA PROCESSOR has 30 days to deal with complaints, but will endeavour to respond to each complaint and claim as soon as possible.

For details see our Complaints Handling Policy

4. Rights of the person concerned and their enforcement

4.1.THE RIGHT OF THE PERSON CONCERNED TO INFORMATION

The DATA CONTROLLER primarily obtains their personal data from the persons concerned, the DATA CONTROLLER makes the following information available to the person concerned upon request:

● the identity and contact details of the DATA CONTROLLER and its representative;

● the contact details of the data protection officer of the DATA CONTROLLER;

● the purposes for which the personal data are intended to be processed and the legal basis for the processing;

● the categories of personal data concerned;

● recipients of personal data and categories of recipients; if any, the information specified in the General Data Protection Regulation in case of transfer of personal data to third countries;

● the duration of the storage of personal data or, where this is not possible, the criteria for determining that duration;

● if the legal basis of the data management is the consideration of interests, then it is the legitimate interest of the DATA CONTROLLER;

● the fact that the person concerned may request from the data controller access to personal data concerning him/her, their correction, deletion or restriction of processing, and may object to the processing of personal data, as well as the person's right to data portability;

● in the case of data processing based on consent, the right to withdraw consent at any time, without prejudice to the legality of data processing carried out on the basis of consent before its withdrawal;

● the right to submit a complaint addressed to the NAIH as a supervisory authority;

● the source of the personal data and, where applicable, whether the data comes from publicly available sources;

● the fact of automated decision-making, including profiling, as well as, at least in these cases, the logic used and clear information regarding the significance of such data management and the expected consequences for the person concerned;

● expressly consents to the processing of the job applicant's personal data as well as to their transmission of such data to legal entities (contracted partners) within or outside the national territory of the country in which the applicant is located and which have a customer relationship with our Company by accepting this declaration, which you do by registering on the website ..... In the case of data transfers abroad, the third country to whose territory the personal data are transferred ensures the appropriate level of protection in relation to the processing of personal data. We do not transmit sensitive data to third parties, either orally or in writing, nor do we create any possibility for third parties to gain access to sensitive data in any way. The data provided for the use of the website is handled

with the voluntary consent of the user and in accordance with this Data Protection and Data Security Regulation. Registration is subject to acceptance of the terms and conditions set out in this document. By registering on the.....page with the purpose of accessing the services required for registration, the job applicant simultaneously accepts the terms and conditions set out in this document.

● due to the technical operation of the website, the start and end times of the user's visit are automatically recorded, and in some cases - depending on the settings of the user's computer - the data of the browser, the operating system and the user's IP address. The system automatically generates statistical data from this data.

● the operator does not connect this data with other personal data, it is used solely for the preparation of website visitation statistics.

● by completing the online Service Information Request form and accepting this document, the prospective customer consents to the processing of the data provided.

● the right to information may be refused only in the cases provided for in Article 14(5) of the General Data Protection Regulation.

4.2. RIGHT OF ACCESS OF THE PERSON CONCERNED

At the request of the person concerned, the DATA PROCESSOR shall provide feedback on whether his/her personal data is being processed. If such data management is ongoing, you will be informed, upon request of the following:

● the purposes of data management;

● the categories of personal data concerned;

● the recipients or categories of recipients to whom or to whom the personal data has been or will be communicated, including in particular third country recipients and international organisations;

● where applicable, the planned period of storage of personal data or, if this is not possible, the criteria for determining this period;

● the right of the person concerned to obtain from the data controller the correction, deletion or restriction of processing of personal data concerning him/her and to object to the processing of such personal data;

● the right to submit a complaint to a supervisory authority;

● if the data were not collected from the person concerned, all available information on their source;

● the fact of automated decision-making, including profiling, as well as, at least in these cases, comprehensible information about the logic used and the significance of such data management and the expected consequences for the person concerned.

The DATA PROCESSOR will make a copy of the personal data subject to data management available to the person concerned upon specific request. For additional copies requested by the person concerned, the DATA CONTROLLER may charge a reasonable fee based on administrative costs. If the person concerned submitted the request

electronically, the information shall be provided in a widely used electronic format, unless the person concerned requests otherwise. The right to request a copy shall not adversely affect the rights and freedoms of others.

4.3. RIGHT TO RECTIFICATION AND ERASURE

At the request of the person concerned, the DATA PROCESSOR shall correct the inaccurate personal data relating to him/her without undue delay, and - considering the purpose of the data management – ensure that incomplete personal data are completed, including by means of a supplementary declaration, if the person concerned so requests.

At the request of the person concerned, the DATA CONTROLLER shall delete the personal data concerning him/her without undue delay, if

● the personal data are no longer necessary for the purpose for which they were collected or otherwise processed;

● the person concerned withdraws the consent on which the data management is based, and there is no other legal basis for the data management;

● the person concerned objects to the processing of his/her data and there is no overriding legal reason for the data processing, or he/she objects to the use of his/her data for direct marketing purposes;

● the handling of the person's concerned personal data is unlawful;

● personal data must be deleted in order to comply with a legal obligation prescribed by EU or Member State law applicable to the DATA CONTROLLER;

● personal data are collected in connection with the provision of information society-related services to children.

The DATA CONTROLLER shall inform all recipients to whom or with whom the personal data have been communicated of any rectification or erasure, unless this proves to be impossible or requires a disproportionate large effort. At the request of the person concerned, the DATA CONTROLLER will inform about these recipients.

4.5. RIGHT TO DATA PORTABILITY

The person concerned shall have the right to receive the personal data provided to the DATA CONTROLLER in a structured, widely used, machine-readable format, and is also entitled to forward this data to another data controller if

● the data management is based on consent or a contract as a legal basis under the General Data Protection Regulation, or

● data management is automated.

● the rules of the General Data Protection Regulation shall be applied to exclude and restrict the application of the right to data portability.

4.6. THE RIGHT TO OBJECT

The person concerned may at any time object for reasons related to his/her own particular situation against data processing carried out for purposes of public interest or legitimate

interest, including profiling. In this case, the DATA CONTROLLER may no longer process the personal data, unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the person concerned or for the establishment, exercise or defence of legal claims.

This right shall be explicitly brought to the attention of the person concerned during the first contact at the latest, and the relevant information shall be clearly indicated and kept separate from any other information.

5. Data storage

Data of job seekers:

DATA CONTROLLER stores the data of registered jobseekers for 2 years. They can request or execute their deletion from their own account at any time. Before the end of the 2 years, they will be informed of the deletion, which they can extend for another 2 years if there is still a common purpose with the DATA CONTROLLER.

Important notes on the data of job applicants:

● The previous business practice is that job applicants apply with a CV with a photo. The Company firmly states that a photograph is not required. In addition, it is not expected that any hobbies and leisure activities should be included in the current CV. The Company does not need the exact address of the job applicants, it is sufficient to indicate the city in order to be able to contact the job applicant with job offers close his/her place of residence.

● Specific data, e.g. religious, racial, political affiliation, gender identity, health-related data, etc. are not requested from job seekers and job seekers are asked to pay special attention to them when writing their CVs and not to upload such data into the Company's system.

● The Company takes a firm stance against discrimination, which is why it avoids requesting data that could even give rise to such a possibility.

● A certificate of good conduct may only be requested for positions prescribed by law or for positions supported by the client's interest test.

● Requesting references from job applicants: only references provided by the job applicant in his/her CV or otherwise may be requested.

Data of Customers and Prospective Customers:

DATA CONTROLLER may store this data based on the relevant Interest Screening Tests on the one hand for legal reasons (customer) and on the other hand for marketing reasons (sending newsletters). These data will be stored either for the period indicated in the relevant legislation, or until unsubscription.

Cookies: browser cookies are used to collect and store the data necessary to measure visitor traffic, identify the logged-in User's server session data (session ID), and provide convenience features. In order to provide a personalized service and facilitate the login process, the system identifies the logged-in User's computer with a "session cookie", which is deleted when the browser program is closed.

If the User closes only the browser window, when the browser window is reopened, the user will be greeted with the logged-in status. STUDIO IN-EX PLC continuously logs the

date and time of the user's visit, the operating system and browser data, the page visited and the IP address for statistical purposes and in order to prevent abuse and to monitor the performance and operation of the service. The logs are stored for 30 days.

Details of employees and subcontractors:

Data will be stored by the DATA CONTROLLER for the period indicated in the applicable laws.

6. Automated decision-making and profiling

A decision based solely on automated data management - including profiling - which produces legal effects concerning the data subject or similarly significantly affects the data subject shall only be used by the DATA CONTROLLER, if

- Necessary for the conclusion or fulfilment of the contract between the DATA CONTROLLER and the person concerned;

- It may be obtained under Union or national law applicable to the DATA CONTROLLER, which also establishes appropriate measures to protect the rights and freedoms and legitimate interests of the person concerned.

- It is based on the explicit consent of the person concerned.

The General Data Protection Regulation applies to the additional requirements for automated decision-making and profiling.

7. Incident management as a data controller

After becoming aware of the data protection incident, the DATA CONTROLLER shall report it to the National Authority for Data Protection and Freedom of Information without undue delay, if possible, no later than 72 hours. The notification, if it exists, shall be made in the form and manner specified by the authority, according to the authority's instructions (for example, on the interface designated by the authority or on hot-line). If the Data Protection Authority does not establish an interface, the mandatory content of the notification shall be provided.

- If the data protection incident is not likely to pose a risk to the rights and freedoms of natural persons, the notification need not be made. This decision will be taken by the CEO, after considering all the circumstances of the case.

- The DATA CONTROLLER shall keep a record of the data protection incidents, indicating the facts related to the data protection incident, its effects and the measures taken to remedy it if the supervisory authority specifies mandatory content elements for the recording of incidents, in which case the incident record table shall be be prepared with this content.

- The DATA CONTROLLER shall inform the person concerned of the data protection incident without undue delay if the data protection incident is likely to pose a high risk to the rights and freedoms of natural persons. This decision shall be taken by the CEO, considering all the circumstances of the case, which he/she makes a note of.

- Exception to the notification of the person concerned if

○ The DATA CONTROLLER has implemented appropriate technical and organizational protection measures and has applied those measures to the data affected by the data protection incident, in particular measures - such as the use of encryption – which render the personal data unintelligible to persons not authorized to access the personal data; or

○ After the data protection incident, the DATA CONTROLLER took additional measures to ensure that the high risk to the rights and freedoms of the person concerned is unlikely to materialize in the future; or

○ Information would require a disproportionate effort, in which case the persons concerned should be informed by means of publicly published information, or a similar measure should be taken to ensure similarly effective information to the persons concerned.

8. Data security regulations

The data shall be protected by appropriate measures, in particular against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction and damage, as well as against becoming inaccessible due to changes in the technology used.

The Company shall consider the state of the art when defining and implementing measures for data security. Among several possible data management solutions, the one that ensures a higher level of protection of personal data should be chosen, unless this would represent a disproportionate burden on the Company.

In order to enforce the data security regulations, the necessary measures should be taken to ensure the security of personal data, both manually processed and stored and processed on computer.

When developing specific protection measures, the following basic principles should be taken into account:

● Awareness: in order to increase trust and confidence in IT systems, everyone who uses them should have at least know security methods and procedures on a basic level.

● Responsibility: the security responsibilities of the owners, supporters and Person Concerned of information systems must be clear and unambiguous.

● Proportionality: security degrees and measures must be appropriate and proportionate to the value and reliability requirements of the protected systems, the costs of enhancing security, and the severity and probability of potential damage resulting from security breaches.

● Risk-based security measures

● Timeliness: security should be reconsidered and updated at frequent intervals in response to changes to changes in the potential risks and consequences of a breach of security. (Risk analysis-risk management)

● Integration: a coherent and integrated security approach is required for all elements of an information system.

● Responsiveness: all participants must work together to prevent damage, breaches of security and respond quickly to breaches.

9. Management of physical hazards

9.1. In order to prevent unauthorized access, the physical protection system must be prepared to prevent unauthorized intrusions, and the operators of the "infocommunication" infrastructure must be prepared to detect and prevent them, as well as to prevent unauthorized use of the devices.

9.2. The current anti-virus client will be installed on each workstation, and periodic updates that are due at intervals (especially with regard to virus definitions) will be downloaded and installed.

10. Protective measures

10.1. Data stored on a computer

10.1.1. Regarding the security of personal data stored on computer and network drives, the provisions of the Information Security Regulations must be applied.

10.1.2. During the automated processing of personal data, the following shall be ensured:

● preventing unauthorized data entry;

● preventing the use of automatic data processing systems by unauthorized persons using data transmission equipment;

● the verifiability and ascertainability of the bodies to which personal data have been or may be transmitted using data transmission equipment;

● the verifiability and ascertainability of which personal data have been entered into automated data processing systems, when and by whom;

● the restoreability of the installed systems in the event of a malfunction and

● a report be prepared on errors occurring during automated processing.

10.1.3. Human risk must be controlled by education and/or legal action.

10.2. Manually managed data

The following measures must be taken to ensure the security of manually processed personal data:

● Fire and property protection: documents held in the archives must be kept in a well-locked, dry room equipped with a fire and property alarm system.

● Access protection: documents in active management on a permanent basis can only be accessed by the relevant administrators. Personnel, wage and employment documents, and documents related to the employee relationship shall be kept in a separate, lockable room.

● Human risk: human risk must be protected through education and legal instruments.

10.3. Guiding documents

Regarding the enforcement of the principles contained and measures set out in this section shall be governed by the relevant internal regulatory documents of the Company, such as the Information Technology Security Regulation.

11. Data Protection Officer

Contact details of the internal data protection officer/data protection officer:

- Név: Veronika Molnár
- E-mail: vera.molnar@in-ex.hu

The internal data protection officer / data protection officer shall carry out his/her duties as defined by law and act as a liaison between the person concerned and the data controller and between the company and the data controller and the company as data processor.

The data controller must answer your questions within 30 days at the latest, but only if you send your request to one of the contact details above.

The internal Data Protection Officer/Data Protection Officer is obliged to verify your identity before providing answers and information, and can only provide general information in the case of anonymous, unverified complaints.

Clause

The Company reserves the right to change its Data Protection and Data Security Regulation. This may occur in particular if the scope of the services is extended or if required by law. A change in data management shall not imply a processing of personal data other than for the purposes for which it was collected.

Budapest, 24 May 2018

STUDIO IN-EX PLC

Cookie information

General information

An HTTP cookie (colloquially just a cookie) is a packet of information that is sent by the server of the website you are visiting to the web browser used by the visitor (e.g.: Google Chrome, Firefox, Internet Explorer, Apple Safari, etc.), and then the browser sends it back to the server for each request directed to the server. The cookies are created by the web server itself via the browser on the website visitor's computer, where they are stored in a separate directory.

The purpose of using cookies

During the provision of its Services, our company uses cookies in order to ensure the proper functioning of the Website and Services, to provide essential and convenient functions of the Website, to enhance the user experience and to provide anonymous statistics.

Cookies used by our company

1. Session cookies

Cookies are essential for the functionality of the Website and some of its functions. In order to facilitate customized service and the login process, the system identifies the logged-in User's computer with a so-called session cookie. If the User only closes the browser window, he/she will receive a logged-in status when the browser window is reopened. These cookies do not allow us to collect any data that could be used to clearly identify the User (personal data). Session cookies are not suitable for marketing purposes, nor for identifying the User's previous web browsing history.

2. Third party cookies

Important: The privacy settings of most browsers allow you to disable third-party cookies. Third-party cookies are downloaded by the User's browser when viewing the Website, not from the Company's web address, but from the third-party domain. Our company uses the following third-party cookies for the following purposes:

- Google Analytics (purpose: to generate anonymous visitor statistics)

- Google AdWords Remarketing (purpose: use of advertising options provided by Google Inc.)

- Facebook Pixel (purpose: to generate anonymous statistics to determine the number of visitors from facebook.com and to use the advertising opportunities provided by Facebook.com)

As our Company does not have the right to control third-party cookies, we ask Users to review the cookie information of these third parties:

- Google Analytics
- Google AdWords
- Facebook

Third-party cookies are returned to the third party concerned when the User views, for example, one of their advertisements or visits their website. With the help of these cookies, the third party (e.g. Google or Facebook) can track the user's entire browsing history with regard to the websites that contain the so-called "third-party" modules (for example advertising module, advertisements).

Regarding cookies and modules from third parties used for the operation of the Website, please review the data management and data protection guidelines of the third parties:

- Google Inc.
- Facebook Inc.

The right to change

Our company reserves the right to modify this Information to the Users at any time (information on the Website) unilaterally. The modified provisions, with the exception of modifications of the User's consent, they become effective for the given User upon the first use after publication on the Website.