Policy for meeting the requirements related to personal data protection at Kontrax AD

1. Purpose

The purpose of this Policy is to ensure the control on collection, processing, and storing of information that contains subjects' personal data.

2. Scope

The Policy is applicable for specific areas, working and/ or requiring the direct fulfilment of specific activities with subjects' personal information.

3. Description of activities

The use of personal information about the employees, clients, and partners, as well as the way of its processing, is an inseparable part of the activity of KONTRAX AD. The company has involved significant human, material, and financial resources for the establishment of personal data collection, processing and archiving system.

The implementation of these requirements aims to:

- Protect the personal data
- Determine the way of processing the personal data in terms of confidentiality, integrity. And availability
- Limit the risk for the activity and the legality
- Maintaining the good reputation of the Company
- Fulfilment of contract obligations.

The protection of the personal information and data, stored and processed by Kontrax AD, is guaranteed in compliance with the requirements of the Personal Data Protection Act, other regulatory documents and/ or contract clauses.

Personal data protection is carried out in accordance to the adopted policy on information protection. These instructions are distributed to all people taking part in the processing of personal information. The documents containing personal data are indexed as "for official use only" as per the policy for "Information Categorization" and are stored by HRD.

"An employee responsible for personal data protection" is nominated in regard to meeting the requirements related to collecting, processing, and storing of personal data accepted as such in way of an order by the Executive Director.

"Personal data" determination:

Kontrax AD defines the personal data categories and subject categories to be processed

Employees:

- Names;
- Personal number;
- Address;

- Telephone;
- E-mail address;
- Identity card and/ or passport data;
- Criminal record
- Health certificate
- Education and qualification
- salary
- length of service
- professional experience
- health status

Clients – Natural persons

- Names;
- Personal number;
- Address;
- Telephone;
- E-mail address;

Clients - Legal entities

- Names;
- Personal number;
- Address;
- Telephone;
- E-mail address;

Job applicants:

Research is carried out on the curriculum vitae of all job applicants, partners or third parties in compliance with the applicable laws, regulations, and ethics. It is in proportion to the business requirements, qualification of information and assessed risks.

The research follows all stipulations of the applicable laws: PDPA and labour legislation.

The following is subject to verification and further processing:

- Verification of applicant's curriculum vitae (for completeness and accuracy);
- Confirmation in regard to stated academic and professional qualification, if possible;
- Independent verification of identity (passport or another similar document);
- The applicants undergo a test for verifying the level of professional experience;
- Interview with essential questions based on the information provided in the curriculum vitae, professional qualification, etc.

Where the job in case of employment or promotion, includes access to the means for processing of information, and if those are used for processing of confidential information, the management may decide to perform more detailed verification for completeness and accuracy of the data presented by the applicant.

When the employee will have access to classified information, then the requirements of the CIPA are applied.

If the applicants are selected with the mediation a specialized agency, the contract signed with such an agency shall clearly state their responsibility in regard to the proper verification of the data communicated, the research and notification procedures to be followed, as well as the way of presenting the personal data information about the subject in compliance with the requirements on personal data protection.

The information about all applicants selected shall be collected, stored and processed by Kontrax AD in accordance with the requirements of the PDPA.

The information about the personal data of non-approved applicants shall not be kept.

4. Purpose for collecting subjects' personal data

Kontrax AD defines the specific purposes for collecting, storing and processing of personal data, as follows:

- Employment relationship,
- accounting,
- clients,
- suppliers,
- advertisement and marketing
- legally determined purposes.

5.1 Kontrax AD in their capacity as a Personal Data Administrator:

Storing of personal data collected is carried out using a specialized software – Aladin, for a period as defined according to an order by the Executive Director, namely:

1. For the entire period of the employment relationship as an employee at Kontrax AD. Data is stored using the specialized software – Aladin. Access to information is granted only to the Payroll Department.
2. For 10-year period after the termination of the employment. Deleted is the information about full names, date of birth, address, length of service of the former employee, bank account provided, insurance number.
3. For 50-year period after the termination of the employment – the information kept refers to the renumeration according to the Accountancy Act, Article 12, para.1. The software used for storing is Aladin.
4. Personal data collected in regard to the fulfilment of a contract, shall not be used for marketing purposes, unless explicitly stipulated in the contract and the personal data subject has granted their consent.

5.2 Kontrax AD in their capacity as a Personal Data Processor

Personal information about clients and partners of Kontrax Ad is collected with the purpose set in contract relations or marketing.
The information about clients/ partners is stored for the period of contract validity, and then it is archived in the specialized software ERP system - Pantheon. Access to this system is granted only to the Senior Management and Commercial Department.
The information about marketing purposes is collected and stored after receiving a prior consent (through the website of Kontrax AD, e-mail, or another proven means) by the counterparty, again in the specialized software – ERP Pantheon. The employees of the following departments – Marketing, Commercial, and Pre-sale preparation, have an authorized access to this information.

Information about the clients in the health care field – general practitioners – name and family name, telephone, e-mail, and UIC, is collected and processed through the specialized software - Liman. The access to this information is limited and granted only for Research and Development Department, Hippocrates support.
Personal data about employees, partners and suppliers is processed only by Kontrax AD.
Change requests; required information and deletion are filed using the attached forms for requesting information, change of information, and withdrawal of provided information by the personal data subject; as well as for forms for notifications in regard to breaches in information security – to the subject of the personal data and to the controlling authority (CPDP). Kontrax AD provides information to the subject of personal data with the content determined by the processing categories, within no later than 7 business days for employees and within 14 business days for partners and clients, after receiving the information request form.
The processed personal data shall not be transferred to third parties or other countries, even though being members of the European Union, without the explicit stipulation in a relevant contract/ annex to contract, and consent received from the owner of the personal data, specifying the reason for this transfer, the time for processing by the third party, and way of storing and deletion of data processed. The control for protection of personal data transferred is on the organization undertaking the responsibility for the processing.
The procedure for change request submission; required information and deletion of personal data transferred to a third party shall be described in the contract/ annex to the contract.

5. Providing and disclosure of personal data out of the organization

The nature of the activity of Kontrax AD is in close relation to the provision of sensitive information, including also information about the personal data of subjects and/ or receiving of such information from the subjects. According to the order by the management and in compliance with the legal requirements set for the companies registered in Republic of Bulgaria, the following main directions are determined:

- To public authorities:
    - National Revenue Agency – full names, Personal number, job position, salary and contract date.
    - National Social Insurance Institute - full names, Personal number, job position, salary and contract date.
    - Ministry of Interior – full names, Personal number, job position.
    - Court authorities, LEO - full names, Personal number, job position
    - Insurers - full names, Personal number, job position
    - Occupational medicine - full names, Personal number, job position
- To personal data processor
    - Physical person who processes the personal data on behalf of the administrator and on order or assignment by the latter – full names, personal number, job position, e-mail.
    - IT company supporting an application software – full names, job position, e-mail.
- To business partners
    - For direct marketing purposes – name and family name, position, e-mail, address of the organization

- Common products and services - name and family name, position, e-mail, address of the organization

After receiving the consent of the personal data subject about its processing, Kontrax AD shall not notify the subject/s of personal data about their work-related exchanges.

In regard to request received for disclosure of personal data from a third party, which is not included in the list or in the additional agreement to the employment contract, or in the annex to the contract signed with a client, Kontrax AD shall notify in person the owner of the personal data about the reason for this request, if not specified.

For changes of the above-mentioned list for exchange of information containing personal data, with third parties, as well as the legal and legitimate reason for this change, Kontrax AD shall inform the personal data subjects in way of letter, but shall not request a new consent for the processing of subject's personal data in regard to performing this change.

6. Storing of personal data by the organization

7.1 Term:

The term for storing of personal data is different for the various activities:

- For data related to salaries – according to the Accountancy Act the data is stored for a period of 50 years
- For data related to clients, partners and accounting records for those, according to the Accountancy Act the data is stored for a period until to the last tax inspection, but not less than 6 years
- For data related to and received in regard to the fulfilment of a project, the term for keeping the data is determined as per the contract signed, or the annex to the contract, but not more than the end of the project.
- For data related to video monitoring, according to the Personal Data Protection Act – up to 30 days, excluding the cases, where a record could be used as a proof before the court.
- Data about users and their clients in "Hippocrates – Cloud" is stored as per the legally determined term.

The term for storing personal data cannot be longer than the above-mentioned terms.

7.2 Processing and protection of data:

According to the type of application and use, the personal data collected by Kontrax AD are processed as follows:

Employees' files:

- Hard copies – employee's file
- automated

Files of job applicants:

- automated

Information about clients:

- hard copy – signed contract
- automated

Information about clients – marketing purposes

- automated

Information about partners

- hard copy – signed contract
- automated

Kontrax AD processes person data using software products, thus minimizing the possibility for incorrectness in the personal information to be processed.
The accuracy of the information itself is a responsibility of the owner of the personal data, and it is their obligation to inform Kontrax AD about any changes.
In case of incorrectness found in the information provided, the processor of the personal data shall inform the owner in timely manner through the available form – notification.
If the incorrectness is a result of technical error or problem, a notification is sent to the official responsible for the personal data protection; it is recorded as an information security incident and solving of this problem is initiated. The owner of the personal data is also informed about the occurred incident.
When the security incident is related to the loss or compromising of personal data, the official responsible shall notify the supervising authority, CPPD, within 72 hours, in way of the available notification form.
Verification about data correctness and their protection is carried out throughout their entire lifecycle.

7.2.1 Work processes related to the processing of personal data

Payroll Department – the specialized software ALADIN is used for the processing of the personal information of the employees. Kontrax AD has signed a contract for maintenance and setup of the program according to the current needs.
For protection of information covering also personal data, there are encrypting mechanisms applied too.

Services Department, Commercial Department – the specialized software ERP system – Pantheon, is used. The access to this system is based on the Policy for access control of Kontrax, with rules and processes described and controlled by the adjoining policies as per ISO 27001:2013.

7.2.2 Requirements for storing and processing of personal data in regard to the workstation of an employee form Payroll Department:

The workstation is stored in controlled conditions, with no access allowed for external persons, and when not used, it is closed in secure areas designated for these purposes.
The information carries are secured against possible damages caused by the environment, such as high heat, direct sunlight, and magnetic field sources.
The threats of the environment for the hardware, such as food, smoke, liquids or humidity, sudden heating or cooling, are avoided.
The employee processing the personal data is not allowed to work with the changed equipment until it is checked and delivered for operation. This does not refer to temporary shifting of mobile computers, which main connections are installed by Information Technologies Service Department.
The employee is trained to protect the electronic equipment and the information contained thereto.

7.2.3 Requirements on storing and processing of personal data in regard to server with

ERP system Pantheon:

The access to information or information systems is based on the requirements of the business and the security requirements (according to ISO/IEC 27001:2013), set in the Information Security Policy and the Passwords Management Policy.
This policy applies the rule – "All that is not explicitly allowed, is forbidden!".

Payroll system Aladin:

The access to information or information systems is based on the requirements of the business and the security requirements (according to ISO/IEC 27001:2013), set in the Information Security Policy and the Passwords Management Policy.
This policy applies the rule – "All that is not explicitly allowed, is forbidden!". The system is located on strictly determined computer protected from network access. The access to data in the system is carried out only by the employee responsible for the Payroll or by its deputy nominated with an order by the Executive Director of Kontrax AD.

7.2.4 Requirements on the storing of personal data on hard copy

Storing of personal data (employee files, job applicant files) is carried out according to strictly stipulated procedure in the Payroll Department. The data is categorized, attached to the relevant files and closed in cupboards od special purpose.
The security of the storing place is determined in the Physical Security Policy.

Storing of contracts, annexes thereto and protocols is done according to the procedures fulfilled as per the requirements of the quality management standard ISO 9001.
Complete information is stored in the ERP system – Pantheon. Access to the system is provided to the senior management and Commercial Department.

7.2.5 Personal data protection

When processing personal data Kontrax AD protects it using encrypting mechanisms and electronic certificates. Kontrax AD does not apply other mechanisms for "masking"/ minimizing of personal data.

7.2.6 Physical security and transfer of personal data

The policy of Kontrax AD includes protection the computer hardware, software, data and documentation against loss, theft, unauthorized access and damages caused by the environment. The physical access to the company premises is regulated by an order of the General Manager. The access rights correspond to the requirements of the Compliance Assessment Policy, i.e. to not contradict the legal and regulatory requirements.
According to the requirements for physical protection of personal data and the places where it is stored, the Physical Security Policy is implemented, where special attention is paid to:

- The access to the premises, where the crucial equipment of the company is located.
- Prohibition for storing of archived materials on redundant media
- Prohibition for storing of dangerous materials (easily combustible materials or aggressive chemicals) inside or in close vicinity to the server room or places for personal data storing.
- Prohibition for entering with photographic, video, audio, or other recording devices inside the special areas, unless special authorization is provided.
- The use of adequate in regard to purpose and capacity fire-alarm equipment, video monitoring and SGE

The transfer of information containing personal data is carried out through encrypted, protected connections with the receiver of this information. If the establishment of such tunnel is not possible, the transfer is done through a courier of Kontrax AD, who has passed a special training.

7. Destruction/ deletion of personal data

The personal data at the Payroll Department are not subject to destruction according to the Accountancy Act, Article 12, para.1, for a period of 50 years.

The personal data in the accounting software, referring to partners, are subject to archiving and has a term of storing of 10 years according to the Accountancy Act, Art.12, para.1. After this period the data can be deleted.

Personal data provided in regard to the fulfilment of a contract, shall be automatically destructed after contract completion, by deleting, if the contract/ annex does not specify otherwise.

Personal data of patients, whose general practitioners use the software Hippocrates – Neo, can be destructed after the expiry of the term of storing:

- Of medical files, as stipulated in the Health Act, amended, issue 24/ 22.03.2019, in force as of 1.01.2020– holders of TEMC and NEMC – 40 years after the last issue. For all the rest – after 5 years.
- Health Act, Art. 132, para. 3 – hospitals under Art.131, para.1, item 2 of the HA (SOHMA with authorization for performing activities related to assisted reproduction) store the information for 30 years.

Regulation №39/16.11.2004 on the preventive examinations and dispensary

- Art. 9, para. 1 – The medical institutions/ hospitals store medical information about the preventive checks and examinations they make, for a period of three years

- Art. 9, para. 2 – The general practitioner stores the medical documentation for all preventive examinations and checks of the patients, including those made in other medical institution, for three years after becoming of age – for children, and for pregnant women – three years after the end of pregnancy.

- Sick sheets – Art. 54, para. 4 of the Regulation on the medical expertise – Cancelled sick sheets are stored for 3 years after the date of their issuance.

- Green and yellow prescriptions – term of storing 1 year according to Art.12, para.1 of Regulation № 4/04.03.2009 on the conditions and procedure for prescribing and provision of medical products

Personal data of doctors is changed/ deleted after filing a request form of the data subject and data processing as per the due order.

Personal information provided on paper is subject to destruction using a shredder, after the expiry of its term for storing or the term of the purpose, for which it was collected.

8. Violations

Failure to follow the leading principles of this policy may result in disciplinary actions imposed by Kontrax AD, depending on the type and seriousness of the violation, particularly if it causes instability or loss for the company and/ or if it is a repeated violation.
The annex to the contract for personal data protection/ agreement for personal data protection (suppliers) defines individually the actions, which the parties may undertake in case of violations found in regard to security and compromising of personal information.

9. Rights of data subjects

According to the European Regulation (EU) 2016/279 every personal data subject has rights as stipulated in the regulation. Kontrax AD follows those requirements and applies them as follows:

- Right of information at the moment of data collection – Article 13 and Article 14 – the data subjects have the right to receive information from the administrators of personal data, yet at the time when the latter collect/ receive the personal data, namely:
  Kontrax AD
  е-мейл: dpo@kontrax .bg

The right of information about personal data is provided only for the person, who is the holder of these data, as follows:

Name, surname, family name, Personal Number, address as per the identity card, phone – personal/ work, bank account, insurance policy. Purpose for request of information – changes and amendments occurred.

Information about personal data requested by a third party, which is not mentioned in the policy, shall not be provided.

- Access right – Article 15 – Kontrax AD shall provide the information requested by the personal data subject, only if the request is filed in compliance with the stipulated procedure and the time period set.
- Right of correction – Article 16 - The personal data subject may request a correction of data if incorrectness is found, as well as in case of need of adding missing information.
- Right of deletion (right to be forgotten) – Article 17 – Kontrax AD accepts the possibility for personal data deletion in the following cases:
  - The personal data is no longer necessary for the purposes, which it was collected for, or processed in any other way;
  - The data subject objects the processing;
  - The personal data was processed illegally;

- Right for limiting the processing – Article 18 – in case of incorrectness found or illegality in personal data processing, and in case of objection by the data subject in regard to the processing of their personal data.
- Right of objection – Article 21 - Kontrax AD shall terminate the processing of personal data in case of:
    - Objection by the subject, unless it is proven that there are solid legal grounds for this processing, which have a priority before the interests, rights and liberties of the data subject, or for establishing, exercising or protection of legal claims.
    - Objection against the purposes of the direct marketing,
    - Objection against applied scientific examinations or statistic purposes, unless the processing is necessary for the fulfilment of a task performed due to public interest.
- Right of claim before a supervisory authority – Article 77 – every personal data subject has the right to file a claim before the supervisory authority - CPPD in Republic of Bulgaria, if they believe that the processing of their personal data violates the stipulations of Regulation EU 2016/679 and the Personal Data Protection Act.
- Restrictions of rights provided – Article 23 refers to the limitations as per the Act on the payroll and the Accountancy Act – the personal data subject cannot require deletion of information related to those.

10. Consent

In order to fulfil the policies of Kontrax AD related to their specific actions, every personal data subject shall sign a declaration for providing their written consent for their personal data processing and storing.

Registers

Kontrax AD maintains the following registers:

Register on the processing activities (of the administrator) - Art. 30, para. 1 of GDPR
Register on the processing activities (of the processor) - Art. 30, para. 2 of GDPR
Register on the requests by the data subjects
Register on the violations

11. Responsible person for data protection

Communication with the Data Protection Responsible in Kontrax AD is possible using the following e-mail address: dpo@kontrax.bg.