Group Policy on Protection of Personal Data

Version 1,
Effective as from 25th May 2018

Table of Contents

Introduction

(1) Regulation (EU) 2016/679 of the European Parliament and of the Council 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**) changing the existing legal regime of data protection and free movement of data enters into force as from 25 May 2018.

(2) As organizations established on the territory of the Republic of Bulgaria and processing data of EU citizens, a number of obligations related to the processing of personal data and the free movement of such data arise for the organizations being members of Victoria Group ("the Group") in accordance with GDPR, the acts regarding the implementation thereof and the national legislation in force.

(3) In view thereof the Group submits to its members this Group Policy on Protection of Personal Data ("Group Policy"), which, together with the appendices hereto, shall be adopted and applied on the level of each individual organization as a minimum standard in processing of data of natural persons and in ensuring the free movement of such data.

Definitions

Personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number [EGN], a permanent or current address, an IP address, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Controller: according to this Group Policy a controller of personal data means any of the organizations being members of the Group and stated in Appendix No. 1, which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data subject means any living being that is the subject of personal data stored by an organization. Such are the guests of the hotels of the Holding Company, the workers and employees of the organizations being members of the Group as well as the employees of the contractual partners of the organizations when the same process their personal data.

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

Profiling means any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyze or predict aspects concerning that natural person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is related to the right of the data subject to oppose profiling and his/her right to be informed as to whether profiling exists, the profiling-based measures and the envisaged consequences of profiling for the person.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. The controller is obliged to report any personal data breaches to the supervisory authority where the breach is likely to have adverse effects on the personal data or the privacy of the data subject.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subjects' wishes by which he or she, by a statement or by a clear

affirmative action, signifies agreement to the processing of personal data relating to him or her;

Child means any person aged 16 or under in case that such age is defined in the national legislation on data protection. The processing of the personal data of a child shall be lawful only if parental or guardian's consent has been obtained.

Third party means a natural or legal person, public authority, agency or body other than the data subject and the controller.

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

Declarations

1. The Group organizations commit themselves to comply with all relevant legal acts of the European Union and the Republic of Bulgaria as a EU member state regarding the protection of personal data as well as the protection of the rights and freedoms of the data subjects whose data are collected and processed by the organizations in accordance with GDPR.

2. Compliance with GDPR is described in this Group Policy and the appendices hereto, together with the procedure and records related thereto.

3. GDPR and this policy, together with the appendices hereto, shall apply to all personal data processing activities described in the record of processing activities of the respective organization, including with respect to the personal data of the guests of the hotels, employees, suppliers and contractual partners as well as any other personal data processed by the respective organization.

4. The data protection officer shall be responsible for reviewing the record of processing activities at least once every two years in view of any changes to the processed carried out by each organization, which are related to the processing of personal data, and any additional legislative requirements. Such record must be made available to the supervisory authority upon request.

5. This policy shall apply for all employees and representatives of the Group members as well as for their contractual partners and other processors of personal data such as, for instance, suppliers, tour operators and outsourced bookkeeping companies. Each violation of GDPR or this Group Policy and the appendices hereto shall be examined by the respective organization as per its disciplinary policy and might constitute an offence as in such case the matter shall be reported as soon as possible to the relevant authorities.

6. The contractual partners and all third parties who work with or for the Group organizations and who have or may have access to personal data must have read, understood and undertaken to comply with this Group Policy.

7. No third party may have access to personal data stored by the Group organizations without having first entered into a data confidentiality agreement, which imposes on such third party obligations which are at least as burdensome as the ones the Group has committed itself to, and which entitles the respective organization to check the compliance with the agreement.

Responsibilities and Roles under GDPR

1. The organizations being members of the Group are controllers and/or processors of personal data under GDPR.

2. All persons who carry out managerial or supervisory roles in the Group organizations shall be responsible for the development and encouragement of good practices of processing, as the responsibilities are specified in the individual job descriptions.

3. The data protection officer being a natural person or a legal entity shall be responsible to the senior management of the respective organization being a member of the Group, and in case that a data protection officer is appointed on a Group level such data protection officer shall be responsible to the senior management of the Group, for the administration of the personal data and shall ensure the compliance with the legislation on and the best practices of data protection. To that end the data protection officer shall:
- develop and implement documents proving the organizations' accountability according to GDPR and the requirements of the Group Policy, together with the appendices hereto; and
- manage the security and the risk in relation to the compliance with GDPR, the Group Policy and the appendices hereto.

4. The data protection officer who shall have the appropriate qualification and experience according to the senior management of the respective organization and/or the Group is appointed to be responsible for the compliance with this Group Policy and is directly responsible to do as much as possible to ensure that the respective organization и/ or the Group as a whole complies with GDPR.

5. The data protection officer shall have some specific responsibilities with respect to the procedures and policies being appendices to this Group Policy, which shall be stipulated in detail in the respective documents and shall apply on the level of the individual organization. The data protection officer shall be the first person to whom questions shall be addressed by the employees, guests of the hotels, workers, contractual partners and the remaining subjects

whose data are being processed within the Group, who want clarifications regarding some aspect of the compliance with the data protection legislation.

6. Compliance with the data protection legislation shall be the responsibility of all employees and representatives of the organizations being members of the Group who process personal data.

7. The employee training procedure shall define the specific requirements on training and knowledge in relation to the roles and responsibilities of the employees of the organizations and the Group as a whole.

8. The employees shall be responsible to ensure that all personal data related to them and made available by them to the respective organization are accurate and up-to-date.

Principles of data protection

Each processing of personal data must be carried out in compliance with the principles of data protection according to the provisions of article 5 of GDPR. The policies, standards and procedures being appendices to this Group Policy aim to ensure compliance with these principles.

Personal data must be processed lawfully, fairly and in a transparent manner

Lawfulness: define a legal basis before you process the personal data. These conditions are often referred to as "conditions for processing", for example: consent.

Fairness: for the processing to be fair the respective organization must make certain information accessible to the data subjects as far as feasible. This applies regardless of whether the personal data have been received directly from the data subject or from other sources.

Transparency: GDPR stipulates some increased requirements regarding what information must be available to the data subjects, which is in the scope of the requirement for "transparency." The transparency requirement includes rules regarding the provision of the information under articles 12-14 to the data subjects. These rules are detailed and specific and emphasize the preparation of the privacy notices in an intelligible and accessible form to be communicated using clear and plain language. The specific information that must be made available to the data subject includes at least:

- the data identifying the respective organization and/or the Group, their contact data as well as the contact data of their representatives;
- the contact details of the data protection officer appointed on the level of the individual organization or for the Group as a whole;

● the purposes of the processing the personal data are intended for as well as the legal basis for the processing;
● the period for which the personal data are kept;
● the existence of the rights to demand access, rectification, erasure or objection to the processing as well as the conditions related to the exercise of such rights;
● the respective categories of personal data being processed;
● the recipients or the categories of recipients of the personal data;
● where applicable, controller's intention to transfer the personal data to a third country and the level of protection ensured for the data;
● any additional information necessary to ensure the fair processing.

Personal data may be collected only for specified, explicit and legitimate purposes

Data received for specified purposes should not be used for a purpose other than the purposes which are formally communicated to the supervisory authority as part of each organization's record of processing activities.

Personal data must be adequate, relevant and limited to what is necessary for the processing:
● The data protection officer shall be responsible to ensue that no personal data which are not strictly necessary for the purposes for which they have been received are collected at the respective organization or at the Group as a whole.
● All data collection forms on electronic or paper medium must be approved by the data protection officer.
● The data protection officer shall ensure that all data collection methods are reviewed at least once every two years to guarantee that the collected data are still adequate and their volume is not excessive.

Personal data must be accurate and kept up to date as all efforts must be made for the timely erasure or rectification
● Data which are stored by the respective organization must be reviewed and updated where necessary. No data shall be stored if one cannot reasonably assume that they are accurate.
● All forms used to collect personal data shall include a declaration by subjects that the data provided are accurate and up to date. Upon material changes to the data in view of keeping them up to date the data subjects shall notify the respective organization or the Group by using the provided contact details.
● The data protection officer shall be responsible to ensure that the entire staff has been trained in the meaning of collection and keeping of accurate data.
● The data protection officer shall be responsible to ensure that adequate procedures and policies on keeping accurate and up to date data are applied by taking into consideration the volume of the collected data, how quickly they could change and any other applicable factors.
● At least on an annual basis the data protection officer shall review the dates of saving of all personal data processed by the respective organization or the Group as a whole by taking stock of the data. The data no longer required in the context of the registered purpose shall be deleted in a secure manner in compliance with the Data Storage Procedure.

● The data protection officer shall be responsible to submit responses to the requests for rectification within one month in compliance with the Procedure for considering requests for exercise of rights of the data subjects. This term may be extended by two more months for complex requests. If the organization decides not to grant the request the data protection officer must respond to the request by explaining his/her reasons and by providing information concerning the right to file a complaint to the supervisory authority and to seek judicial remedy.
● The data protection officer shall be responsible to tale appropriate measures under which if inaccurate or out of date personal data have been transferred to third parties' organizations the latter shall be informed that the data are inaccurate/out of date and should not be used anymore for communication of decisions regarding the respective persons and shall also be responsible to transfer the rectifications of personal data to the third party where required.

Personal data must be kept in a form which permits identification of the data subject for no longer than is necessary for the processing
● Where personal data are kept after the date of processing, they shall be reduced to the minimum in order to protect the identity of the data subject in case of personal data breach.
● Personal data shall be kept in accordance with the storage periods specified in the Data Storage Policy and after the expiration thereof the data will be destroyed in a secure manner.
● The data protection officer must specifically approve the storage of data in excess of the periods specified in the Data Storage Policy by ensuring that the justification is clearly defined in accordance with the legislation on data protection. This approval must be in writing.

Personal data must be processed in a manner that ensures appropriate security
The data protection officer shall make an assessment of the risk by taking into consideration all circumstances related to the personal data processing activities described the record of processing activities kept at the respective organization.

When determining the appropriate security level the data protection officer shall also take into consideration the degree of possible damage or loss that may be caused to the persons if a personal data breach occurs, the consequences of the breach and the possible damage to the reputation.

When assessing the appropriate technical measures the data protection officer shall take into consideration the following:
• password protection;
• automatic locking of terminals in inactive mode;
• removal of rights to access for USB and other media with memory;
• software for virus checks and firewalls;
• rights to access based on roles, including rights to access granted to temporary staff;
• encryption of devices that leave the premises of the organizations such as laptops;
• security of local and broadband networks;

• technologies for increasing the protection of privacy such as pseudonymization and anonymization.

When assessing the appropriate organizational measures the data protection officer shall take into consideration the following:
• the appropriate levels of training at the organization;
• measures that take into account the reliability of employees;
• incorporation of provisions regarding data protection into full-time and/or part-time employment contracts;
• determining disciplinary measures upon violations of the rules on data protection;
• monitoring the staff as to whether they comply with the relevant rules on data protection;
• checks of the physical access to personal data in electronic form and on paper;
• adoption of a "clean desk" policy;
• storage of data on paper in locking fire-resistant cabinets;
• restriction of the use of portable electronic devices out of the workplace;
• restriction of the use of employees' personal devices which are used in the workplace;
• adoption of clear rules on passwords;
• regular creation of backup copies of personal data and storage of media outside the site;
• imposition of contractual obligations on the importer organizations in order that appropriate security measures be taken when transferring data outside the EEA.

These checks are selected on the basis of the identified risks for the security of personal data and the possible adverse effects on the rights and interests of the subjects whose data are being processed.

The controller of data must be able to demonstrate compliance with the remaining principles of GDPR ("accountability")

GDPR includes provisions encouraging accountability as a addition to the transparency requirement.. Each organization being a member of the Group shall demonstrate the compliance with the principles of protection of the personal data by applying this Group Policy on Data Protection and the Appendices hereto, by abiding by codes of conduct, by applying technical and organizational measures as well as by applying the principle of data protection at the stage of designing and by default, by preparing data protection impact assessments of processing activities associated with a high risk for the rights and freedoms of the data subjects in accordance with the Data Protection Impact Assessment Standard.

Rights of the data subjects

1. The data subjects shall have the following rights regarding the processing of data and the data that are recorded regarding them:
1.1. to file requests for subject's access as regards the nature of the information being stored and whom it has been disclosed to;

1.2. to prevent processing that could cause damages or suffering;
1.3. to prevent processing for the purposes of direct marketing;
1.4. to be informed of the mechanism of automated decision-making that will have considerable impact on them;
1.5. to have no considerable decisions made solely by means of an automated process that have impact on them;
1.6. to file lawsuits for compensation if they have suffered damages due to a violation of GDPR;
1.7. to take actions for rectification, blocking, deletion, including the :right to be forgotten", or for destruction of inaccurate data;
1.8. to request that the supervisory authority assess whether a provision of GDPR has been violated;
1.9. their personal data to be made available to them in a structured, commonly used, machine-readable format and the right such data to be transmitted to another controller;
1.10. to oppose any profiling which is carried out without consent.

2. Each organization being a member of the Group shall ensure that the data subjects may exercise their rights in accordance with the Procedure for considering requests for exercise of rights of the data subjects.

Consent

1. The Group organizations understand that "consent" means a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject may withdraw his/her consent at any time.

2. The Group organizations understand that "consent" means that the data subject is fully informed of the planned processing and has expressed his/her consent in a good mental state and without any duress. A consent obtained by force or on the basis of misleading information shall not be a valid reason for processing.

3. There must the active communication between the parties in order to demonstrate an active. In may not be concluded that a consent exists if there is no answer to a message or no opposition to general terms and conditions of an organization.

4. In most cases the consent to processing of personal data is obtained by the Group organizations for the purposes of e-marketing (phone call, SMS or e-mail, including a bulletin) during participants' introduction to programs.

5. Where the Group organizations provide online services for children permission must be obtained from a parent or a guardian. This requirement applies for children under 16 years of age (unless the national legislation stipulates a lower age limit).

Data Security

1. All employees shall be responsible to ensure the conditions necessary for the personal data processed within the scope of the processes, which are carried out at the respective organization and which they are responsible of, to be stored in a secure manner and not to be disclosed to a third party under any conditions unless such third party is explicitly authorized by the organization to receive such information and has entered into a confidentiality agreement.

2. All personal data must be accessible only to the persons who need them on the "need to know" principle. All personal data must be viewed with the highest level of security and must be stored:
• in a locked room with access control, and/or
• in a locker or a locked cabinet, and/or
• if in electronic form, with a protected password as per the company requirements, and/or
• on encrypted (portable) electronic media.

3. Care must be taken to ensure that the screens of computers and terminals cannot be seen by any persons other than the organization's authorized employees.

4. Manual records may not be left at places where they can be accessed by unauthorized persons.

5. Personal data may be deleted or destroyed in accordance with the Data Storage Policy. Manual records whose storage end date has been reached must be destroyed and discarded as "confidential data waste". Hard drives of unnecessary personal computers must be removed and destroyed immediately.

6. Processing of personal data "outside the premises" poses a potentially higher risk of loss, theft of or damage to the personal data. Staff must be specially authorized to process data outside the premises.

Disclosure of Data

1. The organizations being members of the Group ensure that the personal data have not been disclosed to family members, friends, government authorities and, under certain circumstances, the police. All employees must be careful when asked to disclose personal data stored by another person to a third party and shall be obliged to pass special training so that they can effectively cope with such a risk. It is important to take into consideration whether the disclosure of information is related and necessary for the performance of the organization's business.

2. All requests for provision of data for any of these reasons must be accompanied by the appropriate documents and for all disclosure there must be special permissions on part of the data protection officer.

Retention and Destruction of Data

1. The organizations being members of the Group shall not keep personal data in a form which permits the identification of the data subject for no longer than is necessary in relation to the purposes for which the data were initially collected.

2. The organizations being members of the Group may keep data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures in order to safeguard the rights and freedoms of the data subject.

3. The storage period for each category of personal data is specified in the Data Storage Policy.

4. Personal data must be destroyed in a secure manner in accordance with GDPR – data shall be processed in an appropriate manner in order to maintain the security, thus protecting the rights and freedoms of the data subjects. Each destruction of data shall be made in accordance with the Data Storage Policy.

Record of data processing activities

1. The organizations being members of the Group shall introduce a process of taking inventory of data and a data flow as part of their approach to cope with the risks and possibilities within the entire project for compliance with GDPR, by means of preparation of an organization-specific Record of data processing activities which includes:

- the business processes related to processing of personal data;
- the sources of personal data;
- the categories of data subjects;
- the categories of personal data being processed;
- the purposes for which each category of personal data is used;
- recipients and potential recipients of personal data;
- the role of the organization in processing of data.

2. The organizations being members of the Group are aware of all risks related to the processing of personal data.

2.1. Each of the organizations shall assess the level of risk associated with the processing of the personal data. The assessments shall be made in accordance with the Data Protection Impact Assessment Standard and in relation to the processing undertaken by other persons on behalf of the organization.

2.2. Where a certain kind of processing is likely, in particular where new technologies are used, and considering the nature, scope, context and purposes of the processing, is likely to cause a high risk for the rights and freedoms of natural persons, before the processing is carried out the respective organization shall make, after consulting the data protection officer, an assessment of the impact of the envisaged processing operations on the protection of the personal data. A set of similar operations representing similar high risks may be examined in one data protection impact assessment.

2.3. Where as a result of a personal data protection impact assessment makes clear that the respective organization will commence the processing of personal data which might cause damage and/or suffering to the data subjects, the decision on whether the organization may continue must be consulted with the data protection officer.

2.4. If there are serious concerns both as regards the potential damages or suffering and as regards the quantity of relevant data the data protection officer shall escalate the matter to the supervisory authority.

2.5. Appropriate inspections shall be selected and applied in order to reduce the level of the risk related to the processing of individual data to an acceptable level in view of the documented criteria on the acceptance of the risk by the organization and the requirements of GDPR.

Video Surveillance

In cases where the Group organizations carry out video surveillance as an activity related to the processing of personal data they shall store the data for a minimum period determined in the Data Storage Policy. Video surveillance shall be carried out only in the places expressly marked by shortened privacy notices on the basis of organization's legitimate interest in ensuring the security of its employees and property without affecting in any manner whatsoever the rights and dignity of the data subjects (thus, for instance, the organizations shall not carry out video surveillance in toilets, changing rooms, rest rooms and so on).

Appendices

The following documents shall be an integral part of the Group Policy on Protection of Personal Data:

Appendix 1	**List of the organizations being members of the Group**
Appendix 2	**Data Storage Policy**
Appendix 3	**Data Portability Policy**
Appendix 4	**Standard on Assessment of Risk Impact on Data Protection**
Appendix 5	**Notification procedure in case of data breaches**
Appendix 6	**Procedure for considering requests for exercise of rights of the data subjects**
Appendix 7	**Employee Training Procedure**

List of revisions

Version 1, 25 May 2018	Prepared and adopted in accordance with the General Data Protection Regulation