The excerpt from "Personal Data Protection Policy" of Voluum

1. The security of Personal Data means its protection against all dangers in order to ensure business continuity, minimize risk and maximize the return of business opportunities. Security is achieved through the use of numerous technical and organizational measures.

2. Maintaining security of the processed Personal Data is understood as ensuring their confidentiality, integrity, availability and accountability, whereas:
    a. Confidentiality of information – is understood as ensuring that only authorized persons have access to the information,
    b. Integrity of information – is understood as ensuring accuracy and completeness of the information and the methods of processing it,
    c. Accessibility of information – is understood as ensuring that the authorized persons have access to the information and the resources connected with it when it is necessary,
    d. Accountability of information – is understood as every opportunity for Voluum to demonstrate compliance with the rules on the protection of Personal Data, including the assurance of the possibility of assigning in an unambiguous manner the performed activity to a specific person.
3. Voluum undertakes continuous actions to ensure the legality of processing and improving the security of processed Personal Data in its possession, including data entrusted by other subjects on the basis of civil-law contracts.

Technical and organisational measures necessary for ensuring confidentiality, availability, integrity and accountability of Personal Data

1. The security of the Area of Personal Data Processing is provided especially by the following rules:
    a. Only authorized persons, who are also obligated to keep confidential information confidential, including in particular Personal Data processed by Voluum, employees and other persons employed by Voluum or cooperating with Voluum, are entitled to stay in the Area of Personal Data Processing.
    b. Other persons who, as a general rule, do not process Personal Data and therefore have not received appropriate authorization, such as those belonging to technical services, cleaning companies, are obliged to keep confidential information confidential in the scope described in point a. above and may stay in the processing area only with the consent of Voluum and only to the extent necessary to perform their duties, if possible in the presence of a person authorized to process Personal Data in the case of staying in the Area of Personal Data Processing.
    c. The Area of Personal Data Processing is protected 24 (twenty four) hours a day,

7 (seven) days a week by security guards.

d. Access to the Area of Data Processing is controlled with the use of the individual door entry cards. It is forbidden to hand over or lend the cards to other persons. e. Guests report to the Voluum reception where their hosting employee is to be called. The employee is obligated to accompany the guest during their visit in the Area of Personal Data Processing.

f. Voluum shall use technical and organizational measures in order to ensure the protection of processed data appropriately to the threats including external and environmental threats such as fire, flooding, explosion, disasters and other natural hazards through, among others fire protection system and placing extinguishing equipment in suitable and easily accessible locations, applying backup copies and storing them in places ensuring protection against unauthorized takeover, modification, damage or destruction.

2. Securing of paper documents containing Personal Data:

a. Paper documents containing Personal Data are stored in lockable lockers and places inaccessible to unauthorized persons.

b. Access to Personal Data documents is exclusively granted to persons authorised to process Personal Data contained in those documents.

c. Leaving paper documents containing Personal Data at a workplace (desk) is possible only during processing of these documents.

d. Documents containing Personal Data designated to utilization are destroyed in the shredders or in order to destroy them transferred to external entities specialising in Data Erasure. Data Erasure is confirmed using the Data erasure protocol.

3. Protection against data loss caused by power supply failure or disturbances: a. The premises, where Personal Data is processed, have lightning protection system.

b. The IT network is protected against sudden power outages and voltage drop cases by switching on UPS type backup devices for key devices, including servers.

c. Most of the users use laptops, which are not susceptible to power failure or voltage drop.

d. In case of users working on desktop workstations not connected to power supply support systems, those users are obliged to work in autosave mode for the documents they are processing or for other processes if the applications being used have such functionality.

4. Protection against viruses and malware:

a. File resources of workstations, servers and email are vulnerable to viruses and other malware.

b. The basic source of viruses and other malware is the access to Internet

webpages, email and using media with unauthorized software.

c. Voluum has implemented a few security measures against unauthorized access and operation of malware: Firewall – access to the local network from the Internet is protected using firewall and the IT Administrator is responsible for firewall administration, Antivirus software. Virus definition database is updated on an ongoing basis and as soon as new definitions are released by the software producer.

d. The antivirus software performs constant scanning of the open files and email during user's work at the personal computer, which minimises infecting of the system. If a virus is detected, the software automatically repairs the infected file. If removing the virus from the file is impossible, the file is transferred to quarantine.

e. Servers processing Personal Data are installed in the secure server room or entrusted to other providers, to whom Processing of Personal Data was entrusted.

5. The procedure of granting and registering permissions in IT Systems: a. Users are granted the minimum permissions necessary to perform their tasks. b. For a correct authorization, there is a login assigned to the user as well as the individual password determined by that user. Two-factor authorization is required for the systems indicated by the IT Administrator.

c. Users are instructed about the confidentiality of the received password and must not make it available to third persons. Employees must not leave the password printed or written on a piece of paper in a place visible to other employees, co-operators or unauthorised persons.

d. Upon the first logging in to the system, the user is obliged to change the initial password if the password was granted by the System Administrator.

e. The user password should contain at least 8 (eight) alphanumeric characters, including small letters, capital letters, digits and special characters.

f. It is not advised to use names, surnames, nicknames or dictionary words as the content of a password.

g. Passwords kept in the system are encrypted and it is impossible to decipher them using commonly used editors.

h. In the event of a loss of or forgetting an active password it is not possible to retrieve it from the system. In order to give access for the user who lost their password, at the request of that user, the System Administrator grants new password or sends a link which allows to change the password.

6. Inspections, failures and liquidation of equipment and data carriers: a. The inspections and maintenance of devices and equipment involved in securing of Personal Data processing are performed regularly by the IT Administrator or under their supervision.

b. In the occurrence of equipment malfunction, it is unacceptable to forgo the security measures because of the malfunction.

c. Malfunctioning devices are to be repaired on Voluum premises. If equipment's malfunction is serious and requires repairs to be conducted outside Voluum, it is transferred to a third party, if it possible, after the erasure of the Personal Data stored on the disc. In the event that this is not possible, Voluum entrusts the processing of these data after the conclusion of the data processing agreement with the relevant entity.

d. Data carriers should be stored in lockers or in a safe. Access to the place of storage is admissible only to persons authorized to process Personal Data contained on those carriers.

e. It is recommended that the Personal Data stored on a data carrier is encrypted. f. After using a data carrier for operational purposes, the Personal Data saved on it needs to be permanently deleted.

g. Equipment and other electronic data carriers containing Personal Data designated for liquidation are at first deprived of the data with the use of dedicated data erasing software before sending it for liquidation.

h. In justified cases, equipment and other electronic data carriers containing Personal Data designated for liquidation are to be transferred to a third party dealing with physical liquidation of equipment and data carriers. In the event that the equipment and the carriers contain Personal Data, Voluum entrusts the processing of this data after the conclusion of the data provision agreement with the relevant entity.

i. Every Data Erasure and liquidation of data carriers is confirmed with the Data Erasure Protocol.

j. Voluum signs with third parties service agreements including a non-disclosure agreement, which included provisions on confidentiality and security of the data.

7. Other technical measures:

a. The users are forbidden to use unauthorized software. Newly installed software should come only from trusted sources and the fact of installation should be each time consulted with the IT Administrator.

b. IT Systems processing Personal Data ensure accountability of the operations performed on Personal Data by reporting information about the date, scope and person performing a given operation.

c. Personal Data databases and systems are subject to periodic carrying out of backup copies. The IT Administrator is responsible for making and testing backup copies.