FŐVÁROSI VÍZMŰVEK

Policy

Data Protection and Data Security Policy of Waterworks of Budapest Private Company Limited by Shares

July 1, 2012

Contents

1. Aim of Directive

This Policy aims to ensure that Waterworks of Budapest Private Co. Ltd. (hereinafter referred to as Data Manager or Company) complies with Paragraph (3) of Article 24 of Act CXII of 2011 on the right to information self-rule and the freedom of information (hereinafter referred to as the Info Act). According to the cited provision, public utility operators are obliged to draft a Data Protection and Data Security Policy in order to implement the Info Act.

Since the Data Manager is obliged to draft a Data Protection and Data Security Policy as public utility operator, this Policy solely applies to data management performed as public utility operator.

2. Scope of Application

2.1. Related Documents

The Company's contractual documents on utilisation of public utility services

Forms used by clients

Utilisation and data management statement at the web site: www.vizmuvek.hu

Civil Code (Act IV of 1959)

Act CXII of 2011 on the right to information self-rule and the freedom of information

Act CCIX of 2011 on watery utility service and the implementing decree issued upon authorisation thereof

Government Decree 38/1995 (IV. 5.) on public utility potable water supply and public utility sewage collection

2.2. Subject Scope

The scope of this Policy covers every data management by the Company featuring

1. data on persons under client relations with the Company;
2. data on persons formerly under client relations with the Company;
3. data on persons aiming to enter into client relations with the Company;
4. data on persons related to persons under client relations with the Company in a way requiring management of their personal data for the Company's services.

2.3. Temporal Scope

This Policy is effective from 1 July, 2012 until further notice.

2.4. Personal Scope

The scope of this Policy covers the Company and all persons whose data is featured in data management falling under the scope of this Policy, and all persons whose rights or justified interests are affected by such data management.

3. Definition of Terms

The following terms shall be construed as follows for the purposes of this Policy.

3.1. Stakeholder

Any natural entity identified or directly or indirectly identifiable on the basis of specific personal data. In terms of data management falling within the scope of this Policy, stakeholders primarily include the Company's clients and persons whose data the Company manages in relation to public utility services.

3.2. Personal data

Data pertaining to stakeholders – in particular, the stakeholder's name, identifier, or any other piece of information characteristic of stakeholder's physical, physiological, mental, economic, cultural or social trait(s) – and any conclusion that may be drawn from such data concerning the stakeholder.

3.3. Special data

Personal data relevant to race, national or ethnic minority affiliation, political or party standing, religious or other spiritual belief, pressure group membership or sexual orientation, personal data relevant to health condition addiction, and criminal personal data.

3.4. Data of public interest

Any information or knowledge managed by and concerning the activity of or arising in connection with the fulfilment of public tasks of an agency or person fulfilling state or local governmental tasks or other public tasks set forth in legislation beyond the notion of personal data and recorded in any manner or form, irrespective of the method of its management, standalone or collective nature; thus, in particular, assessments extending to scopes of authority and jurisdiction, organisational structure, specialist activity and success thereof, the types of data owned and legislation regulating the operation, and data concerning financial management and contracts concluded.

3.5. Data public due to public interest

Any data beyond the scope of the notion of data of public interest the disclosure of, awareness of or access to which is ordered by law due to public interest.

3.6. Consent

Voluntary and firm expression of stakeholder's intent based on unmistakable information to express unmistakable - comprehensive or transaction-specific – admission to the management of personal data concerning the relevant stakeholder.

3.7. Protest

Stakeholder's statement protesting management of personal data thereof and requesting termination of data management and deletion of data managed.

3.8. Data Manager

The natural or legal entity or unincorporated organisation that independently or collectively determines the aim of data management, adopts and implements the decisions concerning data management (including the means used), or causes implementation by the data processor designated by such entity. In terms of data

management falling within the scope of this Policy, the Data Manager is the Waterworks of Budapest Private Co. Ltd.

3.9. Data Management

Irrespective of the procedure applied, any operation performed on the data or the sum of such operations; thus, in particular, the collection, capturing, recording, sorting, storage, alteration, utilisation, querying, forwarding, disclosing, synchronising or linking, locking, deletion and destruction thereof, and the prevention of further use of such data, the production of photographic, audio or video recordings, and the capturing of physical traits suitable for identification of a person (e.g. finger or palm-prints, DNA samples, Iris images).

3.10. Data Forwarding

Rendering data accessible by a specific third party.

3.11. Disclosure

Rendering data accessible by anyone.

3.12. Data Deletion

Rendering data unrecognisable in a manner in which restoring thereof is impossible.

3.13. Data Marking

Attaching an identifier to data for distinction.

3.14. Data Locking

Attaching an identifier to data to restrict further management thereof ultimately or for a fixed term.

3.15. Data Destruction

Total physical destruction of a data carrier featuring data.

3.16. Data Processing

Performing technical tasks related to data management operations, irrespective of the method and means applied for implementation of operations and the place of application, provided that such technical tasks are performed on the data.

3.17. Data Processor

The natural or legal entity or unincorporated organisation that performs data processing pursuant to a contract concluded with the Data Manager, including contracting pursuant to a legislative provision.

3.18. Data File

The set of data managed in a record.

3.19. Third Party

Any natural or legal entity or unincorporated organisation other than the stakeholder, the Data Manager or the Data Processor.

3.20. Consumer

The natural entity concluding a contract with the Company for public utility services.

4. Entity of and services rendered by the Data Manager

Data Manager is a publicly owned business company providing public utility services aimed at public utility potable water supply falling within the scope of Act CCIX of 2011 on watery utility service and Government Decree 38/1995 (IV. 5.) on public utility potable water supply and public utility sewage collection. Data Manager provides its services within the framework of a contractual legal relationship.

Data Manager is an agency fulfilling a public task.

5. Principles of data management

Data Manager must act in line with the requirements of benevolence and fairness in collaboration with the stakeholders. Data Manager is obliged to exercise rights and fulfil obligations thereof according to their intended purposes.

Personal data shall retain such quality thereof in the course of data management until relationship thereof with stakeholder may be restored. Relationship thereof with stakeholder may be restored if Data Manager is in possession of the technical conditions required for restoring them.

In the course of data management, Data Manager shall ensure the accuracy, completeness and – if required with a view to the purpose of data management – up-to-datedness of data, and that they are only possible to identify with stakeholder until so required for the purpose of data management.

6. Purpose of data management

Data Manager shall manage personal data solely for a specific purpose in order to exercise rights and fulfil obligations thereof. Data management shall comply with the purpose of data management in each and every stage. Data hall be captured and managed in a fair and lawful manner. Data Manager aim to manage only personal data that is indispensable for the purpose of data management and is suitable to attain such purpose. Personal data may only be managed in the extent and for the time necessary for implementing the purpose.

Data management falling within the scope of this Policy may solely serve the purposes below:

1. Contracting with consumer.
2. Provision of services pursuant to a contract concluded with consumer, with a view thereto, identification of point of consumption, testing point of consumption and rendering it suitable for the provision of service.
3. Specification of eligibility for service.
4. Metering services rendered to consumer, ensuring the qualitative and quantitative requirements of services.
5. Metering the object of service, reading off consumption.
6. Specification of payment obligation, invoicing, management of receivables.
7. Management of consumer complaints, reports and claims, recording and investigating such.
8. Enforcement of claims arising from a legal relationship.
9. Direct prospecting, market research and surveys.

7. Legal basis for data management

7.1. Stakeholder's consent

Data Manager shall primarily manage stakeholder's personal data pursuant to stakeholder's consent. Stakeholder may grant such consent:

1. In the contract;
2. On a form;
3. On a separate statement.

In the contract concluded with Data Manager, stakeholder consents to management of all data the management of which is necessary for implementation of the contract. In case the contract may not be implemented without data management, no contract may be concluded in the absence of consent. On the form aimed at contracting, in the General Terms of Contract, and in the Business Policy, Data Manager shall provide information on the scope of data to be managed, the duration of data management, the purpose of utilisation, the forwarding of data, and the engagement of a data processor.

By signing the Contract, stakeholder consents to data management stipulated in the General Terms of Contract and the Business Policy.

In case data management is not necessary for the implementation of a contract, Data Manager shall only manage data if voluntarily supplied by stakeholder. Stakeholder shall be informed on forms on what data need to be managed.

By completing the forms aimed to capture data, stakeholder consents to the management of personal data thereof as stipulated on the forms. Each form shall specify whether data management is mandatory – i.e. is a pre-condition for utilising some service or exercising some right – or is subject to stakeholder's consent.

In case stakeholder grants consent in a separate statement, Data Manager shall offer comprehensive information to stakeholder on the data management in relation to such statement.

7.2. Legislative stipulation

In case the management of personal data is ordered by legislation, data management shall be mandatory. Data Manager shall inform stakeholder accordingly. In case the relevant legislation is valid and effective, Data Manager is obliged to adhere thereto and may not examine the purposiveness, technicality or constitutionality of such legislation.

7.3. Other legal bases

Personal data may also be managed if stakeholder's consent is not possible to obtain or would entail disproportionate costs and the management of personal data is necessary in order to fulfil some legal obligation concerning Data Manager or is necessary in order to enforce a justified interest of Data Manager or some third party, and the enforcement of such interest is proportionate with the restriction of rights pertaining to the protection of personal data. Data Manager shall inform stakeholder if personal data thereof is managed on such legal basis.

If stakeholder is unable to grant consent due to incapacity thereof or some other unavoidable reason, stakeholder's personal data may be managed during the prevalence of such obstacles to consent thereof in the extent necessary to protect the vital interests thereof or of some other person or to eliminate or prevent any direct and imminent threat to persons' lives, physical condition or assets.

If personal data is captured by stakeholder's consent, Data Manager is entitled to manage the captured data without any further consent and even after stakeholder's consent is withdrawn, unless otherwise specified by law, for the purpose of fulfilling any legal obligation pertaining thereto or in order to enforce a justified interest of Data Manager or some third party, if the enforcement of such interest is proportionate with the restriction of rights pertaining to the protection of personal data. Data Manager shall inform stakeholder if personal data thereof is managed on such legal basis.

In cases initiated upon an application or initiative filed by stakeholder, stakeholder's consent in respect of personal data supplied by stakeholder shall be presumed.

8. Scope and management of data

Consumer natural person's identifier data. Management of such data aims at consumer's unambiguous identification and liaising. Data Manager manages the following data of consumer and other contracting parties and other persons affected by services: stakeholder's name, address, mother's name, date and place of birth. In case consumer's data change and this is not reported by consumer, Data Manager shall request stakeholder's data from the personal data and address records in accordance with the stipulations of relevant legislation.

The legal basis for data management is stakeholder's consent – mainly granted in the contract – and legislative stipulation.

Consumer's telephone numbers required for liaising. If supplied by stakeholder, Data Manager shall manage the telephone numbers required for liaising. Stakeholder is not obliged to specify a telephone numbers. In case of consumer groups, Data Manager shall manage the data of the representative of such groups; thus, in particular, the common representative of blocks of flats. Data Manager is entitled to import telephone numbers from lawfully published records, if necessary to contact stakeholder.

Data required for attestation of change in consumer. In case of a change in the identity of consumer, Data Manager is entitled to manage all data required for such change and attestation of such change. Data Manager shall manage a duplicate copy of the document attesting such change. Stakeholder is entitled to cause deletion of data from such duplicate copy that are not required for the attestation of a change in the identity of consumer.

Document duplicate copies and data. Data Manager shall make duplicate copies of certain documents attesting data in order to establish the accuracy of data pursuant to stakeholder's consent.

Data on point of consumption and metering devices. Data Manager shall manage technical and technological data concerning the point of consumption and the metering devices; thus, in particular, the data on property sheets, topographical drawings and plans.

Data on natural persons other than consumer. Primarily, data on the owner of the point of consumption may be managed. In case contracting and service provision is not possible without specification of data on the actual owner, Data Manager shall manage personal data of such owner.

Data on stakeholder consumption, service provision and utilisation. Management of such data is closely related to implementation of contract. Data Manager shall manage data generated in the course of contract implementation; thus, in particular, data concerning consumption, complains, service shortcomings, unlawful actions.

Data on fees and costs payable and paid by stakeholder, data on receivables. Data Manager shall manage all data pertaining to stakeholder's payment obligation from which fulfilment or non-fulfilment of stakeholder's payment obligation may be established.

Data generated in the course of liaising with customer service. This scope covers all data generated by the customer service and during liaising between consumer and the customer service. Data management, in this case, relate to a process launched by stakeholder and relate closely to the contract and to contract fulfilment.

Telephone calls conducted with customer service. Data Manager shall capture and manage pursuant to the stipulations of relevant legislation – primarily in the Act on consumer protection – the audio recording of the telephone calls between stakeholder and the customer service. Stakeholder shall be informed on such recording prior to the commencement of the conversation in every instance.

Data pertaining to other services. In case stakeholder utilises from Data Manager any service other than the public utility service, an additional contractual legal relationship shall arise. In this case, data shall be managed pursuant to the contract.

9. Data management for purposes of direct prospecting, market research and surveys

Data Manager may use stakeholders' personal data for the following purposes upon stakeholders' voluntary consent:

- direct marketing by mail, electronic mail or telephone (including facsimiles and SMS messages);
- contacting for market research and surveys;
- contacting for measuring customer satisfaction and service development.

Use of data pursuant to this Section is subject stakeholder consenting thereto. Such consent shall be voluntary in every case and Data Manager shall not subject contracting thereto. Data Manager reserves the right to allow participation in certain prize-winning and promotional campaigns for individuals having consented to management of their data pursuant to this Section.

Stakeholders may withdraw their consent to data management pursuant to this Section at any time without any reasoning.

In the course of each and every contacting, Data Manager shall inform stakeholders on the possibility of withdrawing their consent.

10. Management of Data Files

Data Manager shall ensure compliance of the method and data contents of records with then current legislation in effect. Data management pursuant to legislation are mandatory, stakeholders may request information thereon. Data Manager shall provide for proper logical separation of data management for different purposes.

Data Manager shall manage electronic and hardcopy records pursuant to uniform principles with consideration given to the diversity of data carriers of records. The principles and obligations pursuant to this Policy shall prevail in respect of both electronic and hardcopy records.

The records featuring client data and those pertaining to services rendered by Data Manager are distinct in order to allow for the separation of data management distinguished by legal basis and purpose. Through the structuring of records, the specification of authorisations and other organisational measures, Data Manager shall ensure that data featured in personnel records are only accessible by employees and other individuals acting within Data Manager's scope of control that so require in order to fulfil their positions and tasks.

Data Manager shall ensure access to the records for third parties involved as data processors providing services to Data Manager in relation to the management of data while enforcing data security requirements pursuant to the stipulations of Section 14.

Data Manager may produce duplicate copies of stakeholder's certain documents featuring personal data with a view to verification of data accuracy.

Data Manager shall store the hardcopy documents of records with a view to data security requirements, and shall provide for safe-keeping thereof.

Data Manager shall operate electronic records by using specifically designed IT software complying with data security requirements. Such software shall ensure that data may only be accessed for specific purposes and under controlled circumstances by persons so requiring in order to fulfil their tasks.

Data Manager shall aim to enforce the principle of data minimum as much as possible in order to allow access by employees and other individuals acting within Data Manager's scope of control to required personal data only.

Management and safe-keeping of data files, access rights and use of data and documentations shall be governed by policies and directives in effect within Data Manager's organisation *mutatis mutandis*. Such policies and directives aim to enforce the principles and provisions of this Policy and relevant legislation – primarily Act CXII of 2011 on the right to information self-rule and the freedom of information.

11. Management of Archival Materials

Data Manager as a business company providing public utility services falls within the scope of regulations concerning protection of archival materials. Pursuant to Act LXVI of 1995 on public documents, public archives and protection of private archival materials, the documents generated at Data Manager qualify as public documents, the retention of which is governed by the cited Act, the document management rules and archival plan issued on the basis of such Act.

Data Manager shall keep a record of the archival materials pursuant to relevant rules even if the purpose of the management of personal data present in the documents have otherwise ceased. In this case, the legal basis for data management shall be the statutory regulations concerning archival materials.

Data Manager shall provide information to stakeholders on regulations concerning the retention of archival materials.

12. Data Security

Data Manager shall provide for data security; to this end, shall take the necessary technical and organisational measures in respect of data files stored on both IT devices and conventional hardcopy data carriers. Data Manager shall provide for enforcing data security rules stipulated in relevant legislation. Data Manager shall provide for data security, shall take the necessary technical and organisational measures and shall put in place the rules of procedures required to enforce relevant legislation, data and confidentiality rules.

Data Manager shall protect data by appropriate measures against unauthorised access, alteration, forwarding, disclosure, deletion or destruction, and accidental termination or damage, and inaccessibility due to alteration of applied technology.

Data Manager shall provide for the enforcement of data security through separate policies, directives and rules of procedures. Data Manager shall provide for the appropriate readiness of relevant staffs in order to enforce data security criteria.

When determining and applying measures serving data security, Data Manager shall consider the then current state of technology. Among the various potential data management solutions, Data Manager shall choose the one offering higher level of protection of personal data, unless that would cause disproportionate difficulties.

12.1. Protection of IT records

Within the scope of IT security tasks, Data Manager shall provide for the following, in particular:

- measures offering protection against unauthorised access, including software and hardware protection, physical protection (access and network security);
- measures offering restoration of data files, including regular safety backups and separate secure handling of duplicates (mirroring, duplication);
- protection of data files against viruses (virus protection);
- physical protection of data files and carriers thereof, including protection against fire, water damages, lightning and other acts of God, and restoration of damages occurring as a result of such events (archiving, fire safety).

12.2. Protection of hardcopy records

In order to protect hardcopy records, Data Manager shall take the measures necessary in respect of physical security and fire safety, in particular.

Employees and other individuals acting within Data Manager's scope of control are obliged to securely retain and protect against unauthorised access, alteration, forwarding, disclosure, deletion or destruction, and accidental termination and damages the data carriers used or held by them that contain personal data, irrespective of the method of capturing such data.

12.3. Regulation of data security

Data Manager shall provide for the enforcement of data security requirements through separate policies and directives. Data Manager's employees and other individuals acting within Data Manager's scope of control shall always proceed in the manner ensuring the highest data security as stipulated in separate policies and directives.

13. Data forwarding

13.1. General rules of data forwarding

Data forwarding may solely take place upon stakeholder's consent or legislative authorisation in any case.

Data Manager shall perform regular data supply for agencies stipulated in legislation at intervals and with scope stipulated by legislation.

In case of occasional data supply relying on legislation, the legal basis for data management must be ascertained at all times and a legal expert must be engaged in case of any doubt. Personal data may be forwarded if the legal basis and purpose are unambiguous and the identity of the addressee of data forwarding is precisely defined. Data forwarding must be documented in any case in a manner allowing for demonstration of its course and lawfulness. Documentation shall primarily be served by properly issued documents requesting and ordering fulfilment of the data supply.

Data Manager is obliged to fulfil data forwarding prescribed by legislation

Beyond the above, personal data may only be forward upon stakeholder's unambiguous consent. For the sake of subsequent demonstration of such consent, it should be put in writing, if possible. Such putting in writing may be omitted if data forwarding is of minor significance with a view its addressee, purpose or data scope. In case of data forwarding subject to stakeholder's consent, stakeholder shall give a statement in awareness of the addressee and purpose of data forwarding.

Data Manager shall log data forwarding in order to establish to whom, on what legal basis and for what purpose personal data had been forwarded. Stakeholders may access the data forwarding log, unless stakeholder may not become aware of the fact of data forwarding pursuant to a legislative provision.

The above prohibitions and restriction apply even upon termination a client relation.

13.2. Regular data forwarding

Data Manager reserves the right to transfer its receivables to a third party by way of concession pursuant to the roles of the Civil Code. Such concession shall alter the

identity of the beneficiary. In case of such concession, Data Manager shall deliver data pertaining to the conceded receivable to the entity becoming the beneficiary by way of concession.

Data Manager shall deliver the personal identifier data and consumption-related data of clients to the Sewage Works of Budapest Private Co. Ltd. collecting and disposing waste water and to the City Hygiene and Environment Protection of Budapest Ltd. Such data forwarding relies on Article 24 of Government Decree 38/1995 (IV. 5.) on public utility potable water supply and public utility sewage collection and on Article 17 of Decree 59/2011 of Budapest City Assembly on mandatory local public utility service pertaining to municipal waste.

Data Manager shall deliver the natural personal identifier data and consumption-related data of clients and the data on metering devices to the Regional Waterworks of the Danube Private Co. Ltd. and to the TÖRSVÍZ Sewage Plant Operator and Service Provider Ltd. upon replacement of metering devices with a view to the fulfilment of tasks pertaining to waste water collection. Such data forwarding relies on Article 24 of Government Decree 38/1995 (IV. 5.) on public utility potable water supply and public utility sewage collection.

Data Manager shall forward data on water meters and points of devices by using an automated water meter reading system to the Distance Heating Operator of Budapest Private Co. Ltd. with a view to invoicing. Data forwarding shall take place upon the relevant consumers' consent.

14. Data Processor

14.1. General rules of data processing

Data Manager reserves the right to engage a data processor in the course of its activities pursuant to permanent or case-by-case assignment. Permanent data processing may primarily take place in order to fulfil administration tasks pertaining to client relations and service provisions, and to maintain the IT system. Engagement of a data processor shall be governed by the provisions of relevant legislation, mainly Act CXII of 2011 on the right to information self-rule and the freedom of information. Data processor may solely be engaged pursuant to a contract in writing.

Upon request, Data Manager shall inform stakeholder on the identity of the data processor and on the details of its data processing activities; thus, in particular, on the operations performed and on the instructions given to the data processor.

The rights and obligations of data processor in relation to the processing of personal data shall be determined by Data Manager within the scope of relevant legislation. Data Manager shall be liable for the lawfulness of instructions concerning data management operations.

Data processor shall be liable for the processing, alteration, deletion, forwarding and disclosure of personal data within its scope of activities and the framework determined by Data Manager. In the course of fulfilling its activities, data processor may not engage any other data processor. Data processor may not adopt any decision on the merit concerning data management, may solely process personal data of which it becomes aware in line with the provisions of Data Manager, may not perform data processing for its own purposes, and is obliged to store and retain personal data according to the provisions of Data Manager.

By devising Terms of Contract offering safeguards and through proper organisational and technical measures, Data Manager shall ensure that stakeholder's rights are not impaired in the course of data processor's activities, and that data processor may become aware of personal data only if indispensable for the fulfilment of its task.

14.2. Specific data processing

The scope of data processors engaged by Data Manager is changing constantly. Data Manager shall provide information on the identity of data processors.

Data Manager shall report the identity of data processors to the data protection records kept by the National Data Protection and Freedom of Information Authority.

Data Manager shall engage the following entities as data processors within the scope of long-term data processing assignments:

- Fee Collecting Holding Private Co. Ltd. – contracting, client services;
- Fee Collecting Print Shop Private Co. Ltd. – invoices, forms, notices;
- Fee Collecting Factoring House Private Co. Ltd. – receivables management;
- Hexaeder Construction and Service Provider Ltd. – technical tasks pertaining to metering devices;
- Self-employed entrepreneurs and business organisations performing meter-reading – consumption reading.

15. Automated individual decision

Decisions based on assessment of stakeholder's personal traits may solely take place through automated data processing if the decision

a) has been adopted during the conclusion or fulfilment of a contract, provided that it was initiated by stakeholder; or

b) is allowed for by an act also establishing measures ensuring stakeholder's justified interests.

Data Manager shall provide information upon stakeholder's application on the methods used in the course of decision-making through automated data processing and on the essence thereof. Stakeholders are entitled to express their positions.

16. Deleting and archiving data

Data Manager shall delete personal data if

a) management thereof is unlawful;
b) stakeholder requests so (save for data management ordered in legislation);
c) incomplete or false data – which state may not be remedied lawfully – provided that deletion is not precluded by law;
d) purpose of data management has ceased or the statutorily stipulated deadline for data storage has expired;
e) ordered by a court or the National Data Protection and Freedom of Information Authority.

Stakeholder may request the deletion of data managed pursuant to stakeholder's voluntary consent. In the absence of stakeholder's application, Data Manager shall delete data if the purpose of data management has ceased. In the absence of any other purpose, Data Manager shall keep a record of the data until the use of data might be necessary in any separate proceedings.

Instead of deletion, Data Manager shall lock personal data if so requested by stakeholder or if impairment of stakeholder's justified interests may be presumed on the basis of available information. Personal data thus locked may be managed until the original purpose of data management prevails that precluded the deletion of personal data. Data Manager shall mark personal data managed thereby if stakeholder disputes appropriateness or accuracy thereof but the inappropriateness or inaccuracy of the disputed personal data may not be established unambiguously.

In case of data management ordered by legislation, deletion of data shall be governed by legislative provisions.

In case of deletion, Data Manager shall render data unsuitable for personal identification. If prescribed by legislation, Data Manager shall destroy the data carrier featuring personal data.

Data carriers qualifying as archival materials shall be governed by Section 11.

17. Data management pertaining to web site of Data Manager

Data Manager shall manage personal data pertaining to the web site www.vizmuvek.hu pursuant to the "Utilisation and data management statement" published on the web site. The statement offers information on all data management pertaining to the web site.

This Policy shall apply to data management by the online customer service *mutatis mutandis*.

18. Stakeholder rights and enforcement thereof

18.1. Right to being informed

Data Manager shall inform stakeholder prior to data management. Such information may be given by Data Manager publishing the brief on details of data management and drawing stakeholder's attention thereto.

Stakeholders may request information on management of their data. Stakeholder may request such information primarily from the customer service or if that is not successful, from the data protection manager.

Data Manager aims to provide stakeholders with details on the data management prior to data management.

Upon stakeholder's application, Data Manager shall provide information on stakeholder data managed and processed by the data processor assigned thereby, on sources thereof, on the purpose, legal basis and duration of data management, on the name and address of data processor and its activities pertaining to data management, and on the legal basis and addressee of data forwarding, in case of forwarding stakeholder's personal data. Upon stakeholder's relevant application, Data Manager is obliged to provide the information within the shortest timeframe reckoned from the filing of such application but within thirty (30) days at the latest. Such information shall be free of charge if the entity requesting such information had not filed an application for information concerning the same scope of data within the subject year. In all other instances, a compensation of costs may be established. The compensation of costs already paid must be refunded if data had been managed unlawfully or if the requesting of information has resulted to corrections.

Data Manager may only refuse to inform stakeholder if authorised by law. Data Manager is obliged to state the reason for refusal of information to stakeholder. In this case, Data Manager shall inform stakeholder on the options of legal remedy.

18.2. Right to correction

Stakeholder may request Data Manager to correct personal data thereof, if featured false. In case of regular data supply taking place on the basis of data to be corrected, Data Manager shall notify the addressee of data supply and shall draw stakeholder's attention to the need to initiate such correction at any other data manager, if necessary.

18.3. Right to deletion and protesting

Save for data management ordered by legislation, stakeholder may request deletion of personal data thereof. Data Manager shall inform stakeholder on such deletion. In case data management pursuant to consent is a condition for establishing or maintaining employment, Data Manager shall inform stakeholder on this and on foreseen consequences.

Data Manager may refuse deletion of personal data if data management relies on legislation and data management is required for enforcing the justified interest of Data Manager. In case of refusal of fulfilment of an application for deletion, Data Manager shall inform stakeholder on reasons thereof.

Stakeholders may protest against management of their personal data as stipulated in Act CXII of 2011 on the right to information self-rule and the freedom of information.

18.4. Enforcement of stakeholder rights

Stakeholders may primarily file their applications for information, correction or deletion with the customer service or the data protection manager.

If Data Manager does not fulfil stakeholder's application for correction, locking or deletion, it shall state the factual and legal reasons for refusal of the application for correction, locking or deletion in writing within thirty (30) days reckoned from receipt thereof. In case of refusal of an application for correction, locking or deletion, Data Manager shall inform stakeholder on the options of judicial legal remedy and of appealing to the Authority.

In case of information, correction, deletion or protest, Data Manager shall proceed in line with the stipulations of applicable legislation. In case of any impairment of rights, stakeholder may request an investigation from the superior of the person acting on behalf of Data Manager and may appeal to the internal data protection manager appointed at Data Manager.

In case of any violation of rights, stakeholder may appeal to a court and may enforce rights pursuant to Act CXII of 2011 on the right to information self-rule and the freedom of information and the Civil Code.

In case of any violation of the right to protection of personal data, stakeholder may appeal to the National Data Protection and Freedom of Information Authority for an investigation thereof.

Data Manager shall be liable for damages caused by any unlawful data management in line with the stipulations of relevant acts.

Data Manager is obliged to compensate damages caused through any unlawful management of stakeholder data or any breach of data security requirements. In respect of stakeholder, Data Manager is also liable for damages caused by the data processor. Data Manager shall be waived from liability if able to prove that damages had been caused by am unavoidable reason beyond its scope of data management. Damages shall not have to be compensated in as much they arose owing to an intentional or grossly negligent behaviour of the party sustaining the damages. Data Manager's general, civil law liability shall be governed by the rules of the Civil Code.

Upon stakeholder's request, Data Manager shall provide detailed information on the options for enforcement of rights.

19. Internal data protection manager and data protection records

19.1. Internal data protection manager

Data Manager as a business company providing public utility services is obliged to appoint a data protection manager in respect of data management performed the as public utility service provider. The internal data protection manager appointed at Data Manager shall proceed in matters falling within the scope of this Policy.

Stakeholders may appeal to the internal data protection manager in all matters falling within the scope of this Policy. The internal data protection manager shall

a) take part and assist in decision-making pertaining to data management and in ensuring the rights of stakeholders;
b) verify adherence to Act CXII of 2011 on the right to information self-rule and the freedom of information and other legislation on data management, and to the provisions of internal data protection and data security policies and data security requirements;
c) investigate notifications received, and shall invite the Data Manager or the data processor to terminate any unauthorised data management, if found;
d) provide for devising an internal data protection and data security policy;
e) keep internal data protection records;
f) provide for training on data protection.

Data Manager shall publish the contact details of the internal data protection manager. Any stakeholder may appeal to the internal data protection manager.

19.2. Internal data protection records

The internal data protection manager shall keep internal data protection records. Internal data protection records shall cover the following for every data management:

a) purpose of data management;
b) legal basis for data management;
c) scope of stakeholders;
d) description of data on stakeholders;
e) source of data;
f) duration of data management;
g) type and addressee of forwarded data, and the legal basis for forwarding, including data forwarding to third countries;
h) name and address of data processor, point of actual data management or data processing, data processor's activities pertaining to data management;
i) nature of applied data processing technology.

The purpose of internal data protection records is to establish data management of which a stakeholder may be the subject of and the typical elements of such data management. Internal data protection records identify data management; however, are no substitute for informing stakeholders in detail.

The internal data protection manager shall ensure access to internal data protection records for all stakeholders.

20. Policy implementation within Data Manager's organisation

When implementing this Policy, the scopes of responsibility and liability of each organisational unit and staff shall be determined by the regulations applying to the Data Manager's organisation, operation and activities. The internal data protection manager shall coordinate the tasks related to the implementation of this Policy.

Data Manager's organisational and operational circumstances are without prejudice stakeholders' rights and to the exercising of such rights. Stakeholders may appeal to the customer service and the internal data protection manager with their questions, complaints and reports related to data management and to rights pertaining to data management. The customer service and the internal data protection manager shall provide for escalating such questions, complaints and reports to the appropriate organisational units and for stakeholders receiving timely responses thereto, and for the necessary measures to be taken.

Data Manager shall provide the contact details of the internal data protection manager and the customer service via the web site.