# "DLV" LTD

## PERSONAL DATA PROCESSING AND PROTECTION CONDITIONS

**Content**

## 1. OBJECTIVES OF CONDITIONS AND TERMS

Objective of this conditions of Personal data processing and protection (hereinafter – **Conditions**) is to establish for DLV:

- organizational events and totality of necessary technical tools that provide honest and legal Personal data processing and use only in provided objectives, its storage, renewal, form of correction and deleting, providing the protection of any physical person rights on their Personal data;

- the fulfilled obligate technical and organizational requirements of the Personal data processing protection, processing physical persons' data and providing the safety of DLV Informational resources and Informational systems;

- the Personal data security violation procedure.

These Conditions have been developed in accordance with the Regulation requirements.

In this document the following terms are used:

| **Term (abbreviation)** | **Definition** |
|---|---|
| Threat | Reasons that do not allow supporting the Informational system safety in accordance with the established requirements of Informational resources Confidentiality, Accessibility and Integrity. Threat of the Informational system safety are intentional (purposely) activities or activities that are made because of incaution or incident that can cause damage, destruction or receiving by such persons that are not authorized or because of whom the access to Informational resources of the system can be violated or impossible. The threat possibility establishes the system Vulnerability. |
| Audit notes | Records from the Informational system memory that are made on different stages of the information processing process to overview these records in appointed order afterwards and track the progress of reviewed process. |
| Highly valuable information | Information, usage of which not in due place, unauthorized change, damage or inaccessibility to authorized persons on any period of time, considerable and prolonged losses can be caused, DLV reputation can suffer and the Personal data safety violation can be done. |
| Authenticity | Quality that certifies that identity of object or resource is such as is declared. |
| Biometric data | Personal data that among to person physical and behavior traits that allow identifying this person uniquely, for example, photographs of face or data of fingerprints. |
| Core HR Data | Name, surname, personal code, birth date, sex, photography (for making a pass), place of residence, phone number, direction of email, number of operating account, personal case (including the information of the work claim (CV; state language certification, diploma's data; reports), work contract, Obligate health check card, assessment of working environment ricks in Employee's working place, function, trainings, activity assessment, career promotion, behavior and discipline data), department units / employer activity, working place data, information about salary, information about illness data and personalized data (SRS), tax data and social insurance data, transport's license plate details, data about Employee's children age (Number of the children's birth certificates of the Employee and the date of issue for additional holiday provision), disability data (for additional holiday provision), in single cases Personal data for making work pass (copy of the stay permit, third country Employee passport data) or visa, for hotel reservation, decisions/ marriage certificates registration data (in case of a |

| | |
|---|---|
| | surname change) |
| Employee | Existing employees (~400), DLV ex-employees and work pretenders. |
| Data Analysis | The data are used in the kind, which analyses behavior and models, and allows drawing a conclusion in each case to improve productivity, competitiveness and / or profit. |
| Data processing person | A term “Person processing the Data” corresponds to established determination in the 8th clause of the 4th article of the Regulation. A society that process Personal data in the name of Data manager. If the society stores or processes Personal data, but does not manage (does not control) Personal data and is processing Personal data, which are based in accordance with the instructions of Data manager, then this society is "the data processing Person". The processing process of the data can include representatives of services (for example, provider of the salary calculation service, IT services provider). |
| Data Manager | A term “Data Manager” corresponds to established determination in the 7th clause of the 4th article of the Regulation. A society that decides why and in what kind (i.e. establishes objectives and tools, by means of which) Personal data is processed. Making a decision about who manages Personal data, it is necessary to answer following questions:<br>- who makes a decision about what information will be stored?<br>- who makes a decision about using the information and the objectives?<br>- who makes a decision about Personal data processing tools?<br>If the society manages and takes the responsibility for Personal data (which is in his disposal) it is Data Manager. |
| DLV | “DLV” LTD is juridical person with single registration Number 40003227719, legal address: 9, Kridenera dambis, Riga, LV-1019 (webpage belonged to DLV: www.dlvbet.lv; DLV gambling halls: “Zilais Dimants”, “Dimats Z” and “Dimanta Bingo”), which acts in status of Personal data Manager. List, in which are enumerated places of provided services of DLV, is available on web-site www.dlvbet.lv. |
| Threats | Any occurrence, because of which DLV can have losses. Threats can be different – different catastrophes, terrorism, loss of the budget financing, communication damages, data damages, mistakes, illegal or harmful activities of employees (also inactivity) and other. |
| Physical protection | Informational resources protection against the Threats that have originated from the physical impact on the information carriers (for example theft, voltage loss, equipment damages etc.) |
| Limited access information | Information of inner turnover, for which Informational resource manager has established circle of admissible persons. |
| Influence | Result of the Information safety Incident. |
| Vulnerability | Imperfection of Informational system, what admits the realization of any established Threat and the safety system influence. |
| Incident | Situation, in which the Information system Threats had a negative influence on Information system’s activity, using its shortcomings. |
| Information resources, | Data files, databases, archives and other information (independently from type of |

| | |
|---|---|
| information | the data carrier). |
| Informational resources' Manager | A person that takes responsibility for Informational resources (their Accessibility, Integrity, Confidentiality, use and the usage consequences) and obligations of which are established in the DLV regulations. |
| Informational system/-s | Data entering, storage and processing in a computerized system that foresees the Users access to get stored data and information in it, or by any form fixed structured Personal data totality, which is accessible, observing appropriate criteria identifying the person. |
| Informational system Administrator | A person that plans, controls and manages the system use and that takes responsibility for its functionality. |
| Integrity | Characterizes, in which size the information is stored and/or passed as full, exact, honest and actual. |
| Special Personal data categories | In the 9th article of the Regulation are established the Personal data kinds, which uncover any of the indicated following information about the person: race or ethnic origin, political opinions, religious or philosophic views or participating in labor union. Special Personal data categories relate also to genetic data, biometrical data (for example, fingerprints or face images), health data, data about sexual life or sexual orientation, also any Personal data, which relate to judgements of guilt or criminal offences. |
| Classification | Appropriation of the level of Confidentiality, Accessibility and Value. |
| Client | a) any physical person that uses, has used, or has a desire to use any providing services of DLV or in any other way is connected to them (including Clients in gaming halls, Clients in an interactive gaming, visitors);<br>b) any physical person that acts in the name of juridical person, provider or other business partner of DLV and stands for such juridical person. |
| Confidentiality | A property, at which the information is not available or is not revealed to unauthorized individuals, systems and processes. |
| Legitimate interests | Originate, if the Personal data processing is necessary in aims of Legitimate interests of Data Manager or Third persons, excepting cases when the data subject interests or the main rights and liberty are more important then such Legitimate interest. Examples of Legitimate interests is the Personal data processing in research aims or for the elimination of criminal offences. |
| User | A juridical or physical person that has made a contract with DLV about the data usage (including the Employees) or that on the base of an inquiry receives the data from DLV or in the order indicated in regulatory enactments. |
| Logical protection | A protection of the Data or the Informational resources that is realized with the help of the software, for example, identifying the Informational system User, verifying the correspondence of his authorities for appropriate IS actions, protecting the information against intentional or accidental change or deleting. |
| Contracting parties | Physical persons (i.e. are not societies) that provides / have provided services to DLV, but not according to the labor contract. |
| Imperfection | Characterizes a system vulnerability category when the concrete Threat realizes, for example, a weak administration system, responsibility, obligations are established inaccurately, an access control is not realized or a control is not total (as physical, as well as logical access), there are no safety conditions of the |

| | |
|---|---|
| | Informational system etc. |
| Personal data | A term “Personal data” corresponds to the established determination in the 1st clause of the 4th article of the Regulation.<br>Any information about an alive physical person that allows directly or indirectly identify this person. The Personal data can include name, surname, personal code, online-identifier, an information about person’s location area or any other information, which is characteristic of this person and which allows to identify a person or makes a person identifiable. The Regulation concerns as to the automated Personal data, as well as to manual systems of the data registration, in which the Personal data is accessible in accordance with concrete criteria. They can include chronological located lists of manual registrations that contain The Personal data.<br>The Personal data that are pseudonyms – for example with the help of a password coded data – can be contained in the area of the Regulation’s activity depending on that, how complicated if to give a pseudonym to a concrete person. |
| Personal data Processing | A term “Personal data Processing” corresponds to the established determination in the 2nd clause of the 4th article of the Regulation.<br>Any activity or activity totality that are made with the Personal data, for example, any kind of Personal data collection, usage, registration, organization, transformation, distribution, elimination, storage or any other activity making the Personal data accessible. The processing can be made or manually, or using automated systems, for example, systems of the informational technologies (accordingly interpreting “to process" and "the processing"). |
| Personal data protection Violation (further – the Violation) | A term “Personal data protection Violation” corresponds to the established determination in the 12th clause of the 4th article of the Regulation.<br>The safety Violation, in consequence of which happens accidental or illegal elimination, loss, transformation, prohibited revelation or access of sent, stored or in any other way processed Personal data. |
| Accessibility | Characterizes, in which volume authorized persons can receive the access to a necessary information no later than at indicated time after the moment of an Information inquiry. |
| Profiling | A term “Profiling” corresponds to the established determination in the 4th clause of the 4th article of the Regulation.<br>Automated Personal data processing to value concrete personal aspects concerned with the physical person to analyze or to foresee productivity, decisions, desires, relation and / or behavior of a person (and correspondingly is interpreted "Profile"). |
| Regulation | The regulation Nr. 2016/679 of European Parliament and European Council (EU) from April 27, 2016 about the protection of physical persons regarding the Personal data processing and free circulation of such data, and in accordance with which is canceled the Directive 95/46/EK (General data protection regulation) |
| Risk (risk) | A probable inability of DLV to realize any his obligations or functions in full volume and qualitatively. In the context of the information safety are considered only those risks that are connected with the Informational systems functionality. |
| Technological resources | Software (realizable program code and configuration files, which ensure Informational systems functionality), computers, computer nets equipment, communication lines and other technical means that are used for information processing, distribution and storage. |

| | |
|---|---|
| Technological resource Manager | A person that takes responsibility for technological resources maintenance and safety. |
| Third person | Any person or society, agency or other organization (which is not the data subject, Data Manager or Person processing Data), who is directly subordinated to Data Manager or Person processing Data, is authorized to process the Personal data. |
| Value | An importance of Informational resource of DLV that is established when valuing possible losses, because of which can arise loss, damage or information receiving by unauthorized persons. |
| Information of average value | Information, usage of which not in due place, unauthorized change, damage or inaccessibility to authorized persons on any period of time, considerable losses can be caused, DLV reputation can suffer and the Personal data safety violation can be done. |
| Public information | Information, which is free for the DLV Employees and any other person access that has inquired this information. |
| Low Risk Information | Information, usage of which not in due place, unauthorized change, damage or inaccessibility to authorized persons on any period of time, DLV does not suffer considerable losses or considerable activity violation does not arise. |

## 2. GENERAL INFORMATION

Data subjects, categories of Personal data processing (also Special Personal data categories) and kinds, aims of Personal data processing, sources, legal basis, Profiling, Personal data distribution, Personal data storage, geographical area the Personal data processing, storage period.

| **Data subjects:** | **Employees** | **Contracting parties** | **Clients** |
|---|---|---|---|
| **Processed Personal data Categories, also Special Personal data categories and kinds** | - Regarding to existing Employees of Core HR Data, email correspondence, photo (video monitoring),<br>Regarding to Employees administrators – a conviction data.<br>- Regarding to ex-Employees of Core HR Data (ex-Employees can request inquiries, characteristics etc.), email correspondence, photo (video monitoring) in less volume, do not storing the illness data and the retirement data (SRS).<br>- Regarding to pretenders to work: name, surname, address, phone number, CV, reviews from previous employers and interviewing notes about pretenders to work.<br>**Personal data special categories:**<br>- **Health data** (Obligate health checks also to investigate work accident (from medical establishments require such information about casualty's health severity (Employee)));<br>- road regulations' violation information;<br>- participation in trade-union organizations /breaking of employee's trade-union contract (in case | Name, surname, personal code, address, phone number, email address, vat number, contract if Contracting party acts at the place, where DLV does video monitoring, also a photo of Contracting party<br>**Special Personal data categories**: are not processed | **Identification data**, for example: name, surname, personal code, date of birth, sex, photo and data of document of identification (for example: passport data, ID card data).<br>**Contact information**, for example: declared and actual place of residence, phone number and email address.<br>**Financial data**, for example: information of the client's bankcard to pay a monetary amount for bet; Client's account number, in case of winning on which it will be paid.<br>**Data that has been received and/or created, realizing obligations provided by regulatory enactments**, for example: data that is based on information requires, which has been received from investigation agencies, sworn notary, administrative tax institutions, courts and legal advisers.<br>**Communication data,** which is collected when a Client visits DLV gaming halls and home pages, where DLV provides services, or communicates with DLV by phone, email correspondence, |

| | | | |
|---|---|---|---|
| | of a contract breaking).<br>Regarding to pretenders to work the Personal data of a Special category is not processed. | | notifications and other communication facilities, for example: social media, data, which is received when a Client visits DLV homepage or communicating with DLV with the help of other canals, also **video records and/or audio records** (photo of a Client making the video monitoring).<br>**Data connected with services**, for example: received services, paid winnings, presented applications, inquiries and complaints. |
| **Processing objectives** | In tax objectives and payment objectives; for realization of administration functions (business strategy, objectives of marketing and advertisements);<br>For prevention of criminal activity or for reveling in relation with a protection of a property and a property that is at DLV disposal, and to protect vital interests of the Employee as the data subject, including life and health;<br>For the observance of legitimate interests of DLV (in the control objectives and improvement of the quality of providing service and/or the Clients' service; to value, stimulate the productivity; for the evidence ensuring against the discrepancy of services and/or of implementation of the contact obligations, also for the evidence ensuring against a possible request, which is based on the delict); | In tax objectives and payment objectives; for realization of administration functions (business strategy, objectives of marketing and advertisements);<br>For prevention of criminal activity or for reveling in relation with a property protection or a usage protection of existing property to protect vital interests of a Contracting party as the data subject, including life and health;<br>For the obligations' realization ensuring, established in the law, DLV as Data Manager and the realization of the applicable regulatory enactments' demands;<br>For the approval and control of the digital canals' access and their activity, the unauthorized access elimination and it's unfair usage, and to information safety ensuring based on the contract implementation, or for | **For the fulfillment of juridical obligations and the identity verification of the Client:** for the realization applied laws regulatory enactments (including, but not the only obligation of DLV is the obligation to make certain of the age of casino, gaming halls and bingo halls visitors, do not allow the minor persons' participation in interactive gaming or interactive lotteries and debar the dependent players on interactive gaming from further participation in gaming (in accordance with the person application no to be allowed to enter gaming halls), also the obligation of DLV is to pay for winnings an income-tax from the population in the order and size established in regulatory enactments; also the obligation of DLV is to pay winning to the player in the order established in regulatory enactments (the third part of the 36th article of the Gaming |

| | | | |
|---|---|---|---|
| | For the aims connected with the DLV homepage (for example, indicating the Employee's contact information);<br><br>For the DLV obligations' realization ensuring and the applicable regulatory enactments realization, established in the law, DLV as Data Manager;<br><br>To sanction and to control the access to digital canals and their activity, to eliminate unauthorized access and its unfair usage, and to the information safety ensure based on the contract implementation, or to realize juridical obligation, or in connection with the Employee's agreement or the DLV legitimate interests to control authorization of the DLV digital services, access and activity;<br><br>To improve technical systems, IT infrastructure, to adapt the service imaging in equipment and to develop the DLV services, for example: testing and improving technical systems and IT infrastructure, based on the DLV legitimate interests to improve technical systems and IT infrastructure;<br><br>For the establishment, realization and defending rights of claim: to establish, to realize, to defend and to cede the claim rights, or to realize juridical obligation, or to realize the claim rights in DLV legitimate interests. | the juridical obligations' realization or in accordance with the Contracting party's agreement, or in legitimate interests of DLV to control the authorization to DLV digital services, access and activity;<br><br>for the improvement of technical systems, IT infrastructure, to adapt services' imaging equipment and DLV services' development, for example: testing and developing technical systems and IT infrastructure, to improve the technical systems and IT infrastructure based on DLV legitimate interests;<br><br>for the establishing, realization and defending the claim rights: to establish, to realize, to defend and to cede the claim rights, or to realize juridical obligation, or to realize the rights of claim in DLV legitimate interests. | and Lotteries Law); also the obligation of DLV is to analyze Clients in the order established in regulatory enactments to present the information to competent institutions to eliminate, to expose, to investigate or to notify about the possible legalization of the criminally earned facilities, terrorism financing, if the Client belongs to the financial sanctions or is a politically significant person), or that legitimate interests of DLV ensure a well-considered risk management and an enterprise management.<br><br>**For the Clients' relations' general management and the ensuring of the services' access and the managing:** for service provision, for the ensuring the data actuality and its accuracy, checking and supplementing data, using external and internal sources, based on the service realization or the juridical obligations implementation.<br><br>**For the protection of the Client's and/or DLV interests:** for the protection of the Client's and/or DLV interests and the quality maintenance of the DLV provided services, and to provide a proof, based on the service realization or, to realize the juridical obligations, or the Client agreement, or in the DLV legitimate interests to eliminate, to limit and to investigate |

| | | | |
|---|---|---|---|
| | | | the unfair or illegal usage of the DLV services and products, or disturbance creation in them, for the inner education or the qualitative services' ensuring.<br><br>For the DLV and/or Client's safety guarantee, the protection of the Client life and health and other DLV and Client's rights, to protect its Clients and the Clients' and DLV actives based on the DLV legitimate interests.<br><br>**For the services' unfair usage elimination and the services' accordance ensuring**: for the authorization of the access control to the digital canals and their activity, the elimination of the unauthorized access and its unfair usage, and for the information safety ensuring, based on the contract realization, or for juridical obligations' realizations or to control the authorization, the access and the activity of the DLV digital services in accordance with the Client agreement or in the DLV legitimate interests.<br><br>For the improving the technical system, IT infrastructure, the adjustment of the equipment of the services' imaging and the DLV services' development, for example: testing and improving the technical systems or IT infrastructure, based on the DLV legitimate interests to improve the |

| | | | |
|---|---|---|---|
| | | | technical systems and IT infrastructure.<br>**For the claim rights' establishment, realization and prosecution:** for the claim rights' establishment, realization, prosecution and assignation, or for the juridical obligations' realization, or in DLV legitimate interests to realize the right of claim. |
| **Sources** | The Employee's Personal data can be collected exactly from the Employee, from the labor contract relations, also form the external sources, for example, employment agencies, enterprises of recruitment of staff members, portals of job applications, SRS, public registers and the public access information. | The Contracting party's Personal data can be collected exactly from the Contracting party, from the labor contract relations, also form the external sources, for example, public registers and the public access information. | The Client's Personal data can be collected exactly from the Client, from the external sources and Client's usage sources, for example, public registers and the public access information. |
| **Rightful principles** | - For the labor contract making and implementation;<br>- For the DLV juridical obligations' implementation in accordance with the regulatory enactments' demands that establish the employer obligations in connection with the Employees (Labor law, regulations of the Cabinet of Ministers Nr.950, dated August 25th, 2009 "Procedures for Investigation and Registration of Accidents at Work", the laws that establish state social insurance, bookkeeping etc.);<br>- For the DLV | - For the contract realization;<br>- For the DLV juridical obligations' realization in accordance with the regulatory enactments' demands, (the laws that establish the bookkeeping etc.);<br>- For DLV legitimate interests ensuring;<br>- In accordance with the Contracting party's agreement. | - For the contract (service) realization;<br>- For the DLV juridical obligations' realization in accordance with the regulatory enactments of Gambling and lotteries (the Gabling and Lotteries Law and the regulations of the Cabinet Ministers Nr. 715 "Order of registration and verification of identity of players of the interactive gaming and lotteries"), Law about the consumer right protection, Prevention of Legalization of the facilities made in a criminal way and Financing of terrorism, law "On accounting", law "On person income tax", law "On taxes and |

| | | | |
|---|---|---|---|
| | Legitimate interests ensuring;<br>- In accordance with the Employee's agreement. | | duties", law "On lotteries and gambling fee and tax", Achieves law and other regulations of the Latvia Republic;<br>- For the DLV Legitimate interests ensuring;<br>- In accordance with the Client's agreement. |
| **Profiling, personalized proposals and automated decision making** | Not conducted | Not conducted | To value established personal characterizations of the Client, for the Client's data analysis and consultation, in the aims of direct marketing, for the automated decision making, for example: for the risk management, for the ensuring providing of remote services, including for the services' supervision to prevent the swindling, and this is based on the DLV legitimate interests, the juridical obligations' implementation, the services' (contract) realization or the Client's agreement.<br>For the improving of the experience of the Client's digital canals usage, for example, adjusting the service's image in the used equipment and, to prepare for the Client the appropriate proposals. If only the Client has not limited the direct marketing regarding to himself, DLV can do the Personal data processing for the general and personalized DLV offers' preparing. Such marketing can be based on the services that are used by the client, how the Client uses the |

| | | | |
|---|---|---|---|
| | | | services, and how the Client acts in the DLV digital canals.<br><br>Profiling that is based on the personalized offers and marketing, which is realized in connection with the DLV legitimate interests, DLV ensures that the Clients can make a choice to use the convenient instrument for the managing theirs privacy setups.<br><br>DLV can also collect statistical data about the Client, including about the typical behavior and the mode of life, on the base of the agricultural demographic data. Statistical data for the segment/profile formation can be received also from the external sources and can be combined with the DLV internal data. |
| **Personal data disclosing** | The Employee's Personal data is disclosed to:<br><br>- server providers;<br><br>- any auditor, financial consultant, collector of debts, legal adviser, sworn attorney, sworn notary and/or sworn bailiff or other Personal data processing person designated by the choice of DLV;<br><br>- Competent specialist for the value of the Labor environment risks because it is necessary to value every Employee's working place;<br><br>- Services' providers about the Employees' education (in the region of the fire safety etc.); | The Contracting party's Personal data is disclosed to:<br><br>- server providers and the other third persons that are connected with DLV in the provision of the provided services;<br><br>- any auditor, financial consultant, collector of debts, legal adviser, sworn attorney, sworn notary and/or sworn bailiff or other Personal data processing person designated by the choice of DLV;<br><br>- Inspection of lotteries and gaming supervision, State revenue service and other institution (for example, law enforcement agencies and institutions of | The Client's Personal data is disclosed to:<br><br>- server providers and the other third persons that are connected with DLV in the provision of the provided services;<br><br>- any auditor, financial consultant, collector of debts, legal adviser, sworn attorney, sworn notary and/or sworn bailiff or other Personal data processing person designated by the choice of DLV;<br><br>- Inspection of lotteries and gaming supervision, State revenue service and other institution (for example, law enforcement agencies and institutions of financial investigations, |

| | | | |
|---|---|---|---|
| | - Inspection of lotteries and gaming supervision, State revenue service and other institution (for example, law enforcement agencies and institutions of financial investigations, courts, out-of-court institutions for the disputes' decision, administrators of bankruptcy and insolvency process);<br>- Other persons that are connected with the services provided by DLV, including the providers of the archiving, postal services etc. | financial investigations, courts, out-of-court institutions for the disputes' decision, administrators of bankruptcy and insolvency process);<br>- Other persons that are connected with services provided by DLV, including the providers of the archiving, postal services etc. | courts, out-of-court institutions for the disputes' decision, administrators of bankruptcy and insolvency process);<br>- Confessed companies on the study of market and public opinion of market (within the framework of the EU) – for canvassing and researches in connection with the offered services of DLV;<br>- Other persons that are connected with services provided by DLV, including the providers of the archiving, postal services etc. |
| **Personal data storage** | Labor contracts, work descriptions, conditions of work order, instructions, other documents (certification of state language, residence permit) in paper format are stored in an office, in folders, in a closed cabinet. Labor contracts formed in electronic format are stored in a computer and in a server in a separate folder "Legal department".<br>Registration books of labor contracts for previous years are accessible as in electronic format (in a computer and in a server), as in paper format (in an office, in folders, in a closed cabinet).<br>Cards of obligate health checks of employees are stored in an office – in a folder, in a closed cabinet.<br>Copies of labor contracts are stored in units (in | Contracts, concluded by parties, in paper format are stored in an office in a closed cabinet. | Client's contracts, filled forms (applications of the Loyalty program) in physical format are stored in folders (in structural units), are located in a cabinet.<br>Client's information is stored in Clients Managing System. |

| | | | |
|---|---|---|---|
| | folders, in a closed cabinet) – for immediate provision to State Inspection of the labor during the time of control (control in relation to an illegal job placement).<br><br>Decrees about Employees movement – as in electronic format (in a computer in a server), as in paper format (in an office, in a closed cabinet), composes the personnel department, are transferred to the accounts department for the processing. Settlement accounts of Employees in paper format are transferred to the accounts department for salary payment. Accountant decrees are stored in the accounts department (in folders, in a closed cabinet).<br><br>With the Employees' Personal data (work candidates) in necessary objectives can familiarize DLV administration or their authorized Employee (including provider of outsourcing of the accountancy and etc.). Names and surnames of Employees can be disclosed to other Employees and Clients of DLV, but other Personal data DLV can disclose only if the agreement of appropriate Employee or candidate is received. | | |
| **Geographical area of the Processing** | Personal data are processed in European Union zone /European Economic zone (EU/EEZ). | | |
| **Storage Period** | Storage period of processed Personal data can be based on the contract, legitimate interests of DLV or applicable regulatory enactment (for example: laws about accounting, archives, legalization of illegally received facilities, limitations, civil rights etc.). DLV stores Personal data in accordance with objectives and intentions of Personal data, as well as in accordance with | | |

| | |
|---|---|
| | requirements of the Regulation and regulatory enactments, including for observing legitimate interests of DLV (for safeguarding evidences in relation with requirements about disparity of services and/or impairment of obligations of the contract, and also for safeguarding evidences in relation with possible requirements outgoing form the delict), DLV stores Personal data ten years from the day of service or contract fulfillment.<br><br>After storage period end DLV deletes files, which contain Personal data. |

## 3. INFORMATIONAL RESOURCES, TECHNICAL RESOURCES AND PERSONS RESPONSIBLE FOR PERSONAL DATA PROTECTION, THEIR RIGHTS AND OBLIGATIONS

Informational resources and technical resources managing:

The administration of DLV in general responds for protection, safety of the information and the process of the optimization of Personal data, which itself or with help of designated person controls reliability of Personal data Processing system.

The administration designates the specialist/-s of Personal data processing and/or the person/-s supporting Informational resources and technical resources, or himself takes the obligation to realize appropriate tasks.

The administration, or the specialist of Personal data processing or the person/-s supporting Informational resources and technical resources designates persons, which answer directly to the specialist of Personal data processing or person supporting Informational resources and technical resources, and which responds for Informational system safety.

The administration in the context of the budget provides persons supporting Informational resources and technical resources the means, which are necessary for safety measures of Informational systems.

Person supporting informational resources:

- in cooperation with person supporting informational resources and (if possible) with information provider do the analysis of risks connected with Informational resources;
- provides measures of Logical protection;
- provides Audit trail of Informational systems, and also its preservation and Accessibility for the control, in connection with Informational systems' safety conditions;
- establishes the order, in which to Informational systems' Users are given access rights to Informational resources and activities with them, and organizes the use control of these resources;
- provides making and saving reserve copies of Informational resources, and also the renewal of Informational resources, if the functionality of the Informational systems was interrupted or impossible because of technical resources' damages and other reasons.

Person supporting technical resources:

- provides measures of physical protection;
- participates in risks analysis, establishes Threats of Informational systems connected with technical resources and evaluates probability of the realization of these Threats;
- provides the renewal of technical resources, if such are damaged;
- provides the renewal of technical resources;

Person supporting Informational resources and technical resources establishes Employees' obligations in the area of Informational systems safety and provides Employees' education and the verification of knowledge in the area of Informational resources and technical resources.

## 4. CLASSIFICATION OF THE PROTECTION OF PERSONAL DATA ACCORDING TO THE DEGREE OF VALUE AND CONFIDENTIALITY

The objective of the classification of the information is to identify all importance of the information at the disposal of DLV and to provide the protection of each informational group according to its classification level.

Persons supporting Informational resources make the Classification of Informational resources by degree of Value, Confidentiality and Accessibility. The Classification of the information is made in connection with requirements of the person supporting Informational resources, if he has established such.

The Classification of the information concerns to all the information independently of information carrier (paper, microfilms, videocassettes, magnetic tape, cassettes, compact disks, hard disks of computers, diskettes and other information carriers).

The Information classify by the Degree of confidentiality, when evaluating its Threats of unauthorized leakage, by following manner:

- Public information;
- Limited access information.

The Information classify by the Level of value, when evaluating Threats of information Integrity, by following manner:

- Highly valued information;
- Medium valued information.

The Information classify by the Level of accessibility, when evaluating its Accessibility Threats. Classifying, establishes also allowed time, by which Informational resources can be not accessible. Classify by following manner:

- the information is accessible always;
- the information is accessible only in working hours.

The information, which is not classified according to Principles of the confidentiality, automatically is considered as the Information of limited access.

All information carriers of Limited access must have appropriate sign about the classification of the information.

## 5. TECHNICAL RESOURCES, WITH WHICH IS PROVIDED THE PROCESSING OF PERSONAL DATA

The processing of Personal data is provided by following technical resources:

- stationary work stations, portative or personal computers;
- servers;
- systems of video monitoring;
- other equipment and software of necessity.

## 6. PROCEDURE OF THE ORGANIZATION OF PERSONAL DATA PROCESSING

Personal data processing takes place in DLV rooms, in rooms, where servers of DLV are placed, and in any place, from which the remote access to Informational resources is provided. Personal data is processed always or of necessity, according to objectives of the processing.

DLV processes Personal data according to the established in the regulatory enactment and only then, if there is at least one of the following conditions:

- the agreement of Personal data subject is received;

- Personal data processing is based on contract obligations of the data subject or on condition of the inquiry of the data subject, Personal data processing is necessary to enter into an appropriate contract;

- Personal data processing is necessary to DLV to realize obligations established in the law;

- Personal data processing is necessary to protect vital interests of the data subject, including life and health;

- Personal data processing is necessary to provide maintenance of DLV interests or to realize state government tasks, for realizing which Personal data were passed to DLV;

- Personal data processing is necessary to realize legal interests of DLV or Third person, whom Personal data were disclosed, observing general rights and liberty of the data subject.

## 7. VIDEO SURVEILLANCE

DLV conducts video monitoring for preventing criminal offences or for disclosing in connection with the protection of the property and vital interests of persons, including the protection of life and health, and also to fulfil of obligations established in lottery and gambling regulatory enactments.

Video monitoring is conducted in and out of DLV gambling halls continuously.

Videos are recorded in computer data carriers, which are located in each gambling hall.

Access to video records is only and centrally from DLV office, remotely connecting to each computer of the gambling hall.

Video records are stored no less than 7 days from the moment of making the record and as far as the capacity of data carrier of each concrete video monitoring system allows. When the capacity of data carrier of the video monitoring system ends, the next data of video monitoring are recorded instead of previous in the same data carrier.

In the context of the disciplinary, administrative or criminal case, DLV saves appropriate video record so long until appropriate case does not end.

Video monitoring is not allowed in a toilet and in rest rooms/zones of Employees.

In each gambling hall in visible place, it is necessary to place writing notification/label, which informs that video monitoring is conducted, indicating in it an objective of video monitoring, DLV company or contact information.

## 8. THE DATA SUBJECT RIGHTS (EMPLOYEE, CONTRACTING PARTY, CLIENT)

Before Personal data processing, DLV provides the information about Personal data processing to:

- Employee, signing appropriate enclosure to a labor contract about Personal data processing;

- Contracting party, included in a contract conditions about Personal data processing;

- Client, familiarized the Client with Privacy notice and Privacy policy.

**Data subject has following rights:**

**1.1.** to request the correction of his Personal data if they are inappropriate, incomplete or incorrect;

**1.2.** to object to his Personal data processing if the use of Personal data is based on legitimate interests, including intentions of the profiling of direct marketing (for example, to receive marketing proposals or participation in surveys);

**1.3.** such rights do not have force if Personal data, deleting of which was requested, are processed also on base of other legal basis, for example, contract or obligations following from appropriate regulatory enactments (for example, Law about legalization illegally received facilities and prevention terrorism financing) or in other cases, established in the Regulation;

**1.4.** to restrict the processing of his Personal data in connection with applicable regulatory enactments, for example, during the time when DLV is valuing if data subject has rights to his data deleting;

**1.5.** to receive the information if DLV processes his Personal data and, if so, then receive the access to them and receive the information, how are they processed and to whom are transferred;

**1.6.** to receive his own Personal data, which he has provided and which are processed on base of implementation of the agreement or the contract in paper format or in any frequent used electronic format and, if possible, transfer such data to other representatives of services (portability of the data);

**1.7.** to recall his own agreement of processing his own Personal data if Personal data are provided to DLV on base of the agreement of data subject;

**1.8.** not to be fully subordinate to an automated decision-making, including profiling, if such decision-making has legal consequences or, which by similar manner visibly influence data subject. Such rights do not have force if the decision-making is necessary to enter a contract or to fulfill a contract with data subject, if decision-making is allowed according to applicable regulatory enactments or, if data subject has given his obvious agreement;

**1.9.** to lodge a complaint about Personal data use in State inspection of the data (www.dvi.gov.lv), if data subject considers, that the processing of his own Personal data violates his rights and interests in connection with applicable regulatory enactments.

**Rights, which person <u>CANNOT</u> use** (with "X" are marked rights, which physical person (data subject) CANNOT use. Cells WITHOUT "X" are rights, which physical person (data subject) CAN use):

| Base to Personal data processing: | Rights to deleting the data | Rights to data transportation | Rights of objection |
|---|---|---|---|
| **Agreement** | | | X<br><br>but rights to recall the agreement |
| **Contracts** | | | X |
| **Legal obligation** | X | X | X |
| **General interests** | | X | X |
| **On the instructions of the state institutions** | X | X | |
| **Legitimate interests** | | X | |

**9. Order, in which DLV provides the Data subject with guaranteed rights and safety events of Personal data**

**Ensuring the Data subject rights.**

*Demands of Data subject:*

If from the Data subject is received a demand to give or to disclose Personal data of the data subject, at disposal of DLV, such demands considers member of the board of DLV or his designated person, and appropriate Personal data can be given or can be disclosed only by member of the board of DLV or his designated person, if such disclosure or transfer is based.

To protect Personal data against illegal disclosure, DLV, receiving the demand from the data subject about data providing or about realizing other rights of the data subject, is convinced in the identity of the data subject. For this objective DLV is entitled to request from the data subject the indication its Personal data, comparing if indicated data of the data subject concur with appropriate Personal data at disposal of DLV. Making this verification, DLV also can send a control notification on telephone number and email indicated by the data subject (messages or by way of email), with the request to make the authorization. If the procedure of verification is not successful (for example, indicated data by the data subject do not coincide with Personal data at disposal of DLV, or the data subject did not authorized by sent message or email notification), DLV will be obliged to establish that the data subject is not the subject of requested Personal data and will be obliged to deny appropriate submitted demand.

Having received the demand of the data subject about execution of any rights of the data subject and successfully have made aforementioned procedure of verification, DLV undertakes to without delays, however in any case no later than during one month from receiving the demand of the data subject and procedure of verification end, provides the data subject the information about activities, which DLV has done according with the demand, submitted by the data subject. Taking in account complication of the demand and the quantity, DLV is entitled to extend the one month's period by two more months, informing about this the data subject until first month end and indicating the reason of such prolongation. If the demand of the data subject was submitted with help of electronic instruments, DLV gives the answer also with the help of electronic instruments, excepting cases when this is not possible (for example, because of large data size) or if the data subject has asked to answer in other manner.

DLV is entitled to deny satisfying the data subject demand with a motivated answer if the circumstances established in regulatory enactments are fixed, or is not possible to certain in the data subject identity, informing about this the data subject in writing. If demands of the data subject obviously are not based or excessive, particularly because of their regular repetition, DLV as Data Keeper can or: a) to require a reasonable payment, taking into an account the administrative expenses that are connected with the provision of information or communications, or fulfillment of requested activities; or b) refuse to fulfill the demand.

*Demands of third persons:*

If from state institutions or self-government or Third person, who are not Employees, Contracting parties or Clients, is received the request to give or to disclose Personal data, at disposal of DLV, such requests considers member of the board of DLV or his designated person, and appropriate personal data can give and can disclose only member of the board of DLV or his designated person if such disclosure or transmission is based.

In any case if the Employee of DLV does not know, how to act – can or cannot disclose some information – the Employee needs to consult with the member of the board of DLV or with his designated person and, the Employee can act in appropriate case only as such as the member of the board of DLV or his designated person has instructed.

DLV, transmitting Personal data, ensures the saving of the information about:

- Time of transmission of Personal data;
- Person, which has transmitted Personal data;
- Person, which has received Personal data;
- Personal data, which have been transmitted.

**Personal data safety measures.**

To protect Personal data against unauthorized access, accidental loss, erasure or damage, DLV uses measures of physical safety: closed card indexes, which contain Personal data; closed offices / rooms with Personal data.

DLV uses safety measures to guarantee the safety of equipment and / or files against unauthorized access, accidental loss, erasure or damage: authorization, archiving, encryption, access of Users, regulation of actions, SSL certificates, firewall.

DLV uses other safety measures to protect Personal data against unauthorized access, accidental loss, erasure or damage: rights of limited access to Personal data (based on the necessity to know); reliable erasure a waste of documents of confidential information (as in paper, as well as in electronic format), education of employees.

Processing Personal data in Informational system, the access to Personal data, technical resources and documents is provided only to authorized persons.

The administrator of Informational systems in cooperation with person supporting Technical resources has rights to make an auditing of Users' actions. Such audits can contain the realization of an auditing of User actions (including attended internet resources), an analysis and a request of additional information about realized activities.

In the context of the supervision of Information systems use:

- Person supporting Technological resources ensure that notations of the Auditing are formed about Informational systems, which contain classified Informational resources, and activities in the computer net, in which is the access to Informational systems, which contain classified Informational resources. In the auditing notation are inserted all dates and time of successful and unsuccessful cases of a connection, and also a code of the User (including person supporting Technological resources) and other methods of the authentication;
- Person supporting Technological resources provides the integrity of notation of the Auditing and regularly composes records of reserve copies of the Auditing data in accordance with rules of these conditions;
- Person supporting Technological resources regularly controls all activities of Informational systems, but pays special attention to the control of activities of Informational system, which contains classified Informational resources. For this objective, the person supporting Technological resources by his choice uses special control programs or computer systems, establishing intrusion.

Person supporting Technological resources controls at least following cases:

- repeated unsuccessful connection to Informational system;
- attempts to connect to Informational resources, to which the User is not authorized to connect;
- the use of Informational systems in unusual time, for example, outside working hours;
- repeated attempts of User code use, which already has been declined;
- appropriation and use of privileged codes of the User;
- unauthorized change of software configurations and inadmissible installation of the software.

The control of viruses of Informational systems:

- Person supporting Technological resources establishes the order and makes events for the prevention of virus activities in the computer of Informational systems;
- For the prevention of virus activities, uses specially provided software for this objective. Files that have determined as viral without delay renews as soon as the developer proposes files for the renewal;
- Person supporting Technological resources regularly controls of anti-viral programs to make sure in its workability and to discover new files, determined as viral.

The protection of personal and portative computers:

- Proprietor of the information establishes, which information is allowed to store on personal or portative computer (further in the text – **personal computers**). In portative computers, which are used outside working rooms of DLV, store only that information, which is necessary in established time to established User of the computer;
- In personal computer establish and use only that software and with that configuration, which has determined by the person supporting Technological resources. Functionality of personal computer is limited to the level of functions, which are necessary for work needs;

- Personal computer, staying unattended of the User, turns off, using the background with password, special function of the disconnection or other method, which allows to continue the work with personal computer only then if is done the authentication of the User;

- Person supporting Technological resources establishes the order, in which for work needs Employees use belonged to them computers and in which use computers outside workrooms of DLV. Such order cannot be decreased on the level of the protection of established Informational resources.

The protection of computer net:

- Person supporting Technological resources develops and maintains the scheme of computer net, in which are shown equipment and provided services connected in computer net;

- data flow between the local computer net and outer computer net admits only those services, which are necessary for DLV function realization, for this objective the systems of firewall are used;

- Person supporting Technological resources regularly checks the existence of all outer connection and makes sure that there is only those connections, which correspond to DLV work requirements and that reserve connections work;

- Connection to Informational systems from logically remote place is protected, using cryptographic tools with the password of the User so to confidently determine the Authenticity of the User.

DLV by necessity realizes additional measures of Logical protection, depending on classification level of resources of Informational system.

DLV realizes equal measures of Logical protection for classified Informational resources independently of storage manner of the data (including diskettes, paper documents, audio cassettes etc.).

DLV in cooperation with inner representatives of informational technology services:

- establish responsibility demands of involved persons, confer to Users temporary accounts, managing changes and other safety demands of Informational systems;
- coordinating with proprietors of the information, confers to outer representatives of informational technologies the access rights to resources of Informational systems only in the ambit that is necessary for obligations realization;
- establish limitations of information distributing.

If DLV decides to entrust the maintenance of Informational systems to outer representation of services, he must ensure the safety level of Informational systems, which is no less than established in these conditions. DLV must familiarize the outer representative of services with safety demands of Informational systems established in these conditions. The order of Personal data processing and the access level establishes roles of Users of Informational systems.

## 10. PASSWORD STRUCTURE, THE ORDER OF ITS USE AND THE ACCESS

To each User of informational resources is conferred a username(s) (identifier(s)) of Informational system and a password, and also established access rights. The User of Informational system has responsibility for the use, the preservation and non-distribution of the conferred access name (identifier) and the password.

Access rights confirms the appropriate proprietor of Informational resources. According to a claim of Informational resources proprietor, the administrator of Informational systems gives the access to the User to all Informational systems indicated in the confirmation.

The proprietor of Informational resources must inform the administrator of Informational systems about those Employees, which discontinue labor relations with DLV. The proprietor of Technological resources after receiving of this information immediately annuls all access rights of appropriate Employee of DLV to Informational systems' resources.

The User of Informational system has responsibility of actions, which are done, using his username (identifier). The Authenticity of the User of Informational system establish to assure that the user of the username (identifier) is its authorized proprietor. To establish the Authenticity are used passwords. After entering the username (identifier) and the password, the User of Informational

system can use resources of Informational system in accordance with established access rights.

The password constitutes from letters, numbers and signs combination and its length cannot be shorter than eight symbols. How the password cannot be used the data identifying the person (for example, Personal data, automobile number, names and surnames of relatives, names that are connected with the working place or that are used there frequently).

When the User of Informational system is entering the password, it must not be seen for reading on the computer's screen.

The User of Informational systems must change the password at least once in three months. The Administrator of Informational systems must guarantee:

automatic request of the password change for the User, for the first time registering in the net;

automatic request of the password change each three months;

the systems' blockage on time to 1 hour if the User five times in a row has entered incorrect password or username.

The User of Informational systems must memorize the password. Passwords in writing is allowed to store only in a closed safe.

If are aroused suspicions that the password has become known by other person, the User of Informational systems immediately notifies about the Incident the proprietor of Informational resources, the proprietor of technical resources and the administrator of Informational systems.

It is not allowed trying to know passwords of other Users, excepting cases when this is necessary to the administrator of Informational systems to the fulfilling his third obligations. After the end of mentioned works the User of Informational systems changes the password.

On the screen must be set the screensaver with the activation password. It must be activated automatically, if within five minutes the User has not made any activities.

## 11. MEASURES, WHICH ARE REALIZED FOR THE TECHNICAL RESOURCES PROTECTIONS AGAINST ACCIDENTS, AND TOOLS, WHICH ASSURE THE TECHNICAL RESOURCES PROTECTION AGAINST INTENTIONAL DAMAGE AND DO NOT ALLOW THE RECEIVE

DLV realizes measures of the physical protection of Informational systems, which protect them against non-wishful factors of the environment (fire, floods, fluctuation of temperature etc.), technical (inappropriate supply of electricity etc.) and human factors (intentional or unintentional damages, theft etc.).

Physical protection of servers:

- DLV assures that all Informational systems are exploited with the limited access in closed rooms, Physical protection of which assures only the access of authorized persons, or assures physical protection of servers, in order to they cannot be turned off, moved, damaged or non-authorized changed its configuration. Server rooms are placed in rooms of the edifice, in which the realization of Threats is less likely;

- Unauthorized persons, including representatives of outer services, in server rooms can bear only accompanied by authorized persons;

- Depending on possible loss amount, DLV assures sufficient protection of servers and server rooms against physical Threats (including against inappropriate climate conditions, fires, floods, interruption of supply of electricity, intentional damages), in case of necessity equipping with security and fire signalization, automatic system of fire-fighting, installing equipment of alternative supply of current and equipment of air-cooling.

For the net infrastructure (including for net communication equipment, cable nets) DLV ensures sufficient physical protection, placing it in such way that the unconnected with DLV persons can not get an unauthorized access and insensibly access, or make its damage, also DLV employees and visitors can not get an unauthorized access and damage it, or accidentally damage it by inadvertence.

Physical protection of working stations:

- The working place of Technical resources' Manager is separated in the limited access rooms;

- Working stations are used in accordance with established demands of the producer, and use equipment of continuous supply of electricity, if is found that the rick of violations of supply of electricity is unacceptably high.

Physical protection of portative equipment:

portative computers are used in accordance with established demands by the producer;

DLV does the registration of the circulation of portative equipment to establish, which person uses appropriate equipment.

Physical protection of data carriers:

- DLV realizes necessary safety measures for the physical protection of all data carriers independently of its kind (including dismantled disk equipment, paper printings, fax printings, diskettes, optical disks etc.);
- Data carriers, which contain resources of Informational systems without special temporary limit can use and move only, authorized Employees of DLV, who have the access to resources of Informational systems. Resources of Informational systems, which are not necessary to use or move, are stored in rooms of DLV in places that are provided for them. If is necessary to annihilate data carriers, the proprietor of Technological resources controls and ensures its annihilation;
- In the context of the protection of data carriers, DLV realizes the physical protection of input and output data equipment, eliminating unauthorized use – equipment of printers do not place in places of public access, do not allow outer activities of data carriers, if they are not necessary for obligation realization of Employees;
- It is prohibited to leave data carriers with classified Informational resources in unsafe (for example, public access) places;
- If is envisaged the annulment of data carrier containing classified Informational resources, then this is realized so that the renewal of existent in it data will not be possible.

In case of necessity, DLV does additional measures of physical protection depending on the level of classification of resources of Informational system. Measures of physical protection of Informational systems are done systematically, not admitting the situation when resources of Informational systems are located outside of the rooms of limited access without the control of authorized Employees of DLV. DLV regularly does the control of measures of physical protection.

Reserve copies of the data are made in accordance with the procedure, established by the member of the board of DLV.

In case of any Incidents, for example, theft of data carriers, in case of loss, appropriate Employee immediately informs the proprietor of Technological resources and Informational resources, who does all necessary measures for data protection.

## 12. THE ORDER OF INFORMATIONAL CARRIERS' STORAGE AND ANNULMENT

In case of the closing of Informational system or before the annulment of informational carriers, responsible person deletes the content of the information, content of databases, also all other connected files.

If it is necessary to delete the data from Informational system, DLV assures full data deleting from Informational system so that it will not be possible to renew it.

## 13. RIGHTS, OBLIGATIONS, LIMITS AND RESPONSIBILITIES OF THE PERSONAL DATA USERS

Users of Informational systems can use appropriated resources of Informational systems only

for realization of work obligations and can process Personal data only in accordance with it processing objectives and for the realization of work obligations.

The User of Informational systems has responsibility for actions, which are done, using his username (identifier). Authenticity of the User of Informational systems are established to ensure that the user of the username (identifier) is its authorized proprietor. For the establishment of the Authenticity are used passwords. After entering the username (identifier) and the password, the User of Informational system can use resources of Informational system in accordance with established access rights.

The User of Informational systems must memorize the password. The password is allowed to store in writing only in closed safe.

It is prohibited trying to know password of other Users, excepting cases when this is necessary to the administrator of Informational systems for the realization of his direct responsibilities. After mentioned works ending, the User of Informational systems changes the password.

When labor relations of the User of Informational systems with DLV end, the administrator of Informational systems annuls all access rights to resources of Informational systems.

Using resources of Informational systems, the obligation of the User of Informational systems is an immediate notification of the administrator of Informational systems in following cases:

- if are aroused suspicions that other persons have learned the password of the User;
- received email messages of incomprehensible origin (for example, unknown correspondents, especially indicated letter subjects);
- if are aroused suspicions that the computer is infected with a virus, also turn off the computer;
- if are aroused suspicions about the damage of computer equipment, also immediately turn off damaged equipment;
- noticed the diversion of the computer or Informational system;
- if it is necessary to change the placement of computer equipment;
- to read notifications, sent by the administrator of Informational system, and to realize indicated activities timely;
- to get to know with instructions and recommendations, included in the catalogue of general use;
- to delete regularly email letters needless for work;
- do not disturb the update process of the antivirus program;
- to look after so that in the computer necessarily was activated backscreen with the password protection. Backscreen must activate automatically if the User within the five minutes did not made any activities.

To the User of Informational systems is prohibited:

- to use resources of Informational systems to distribute or store information unconnected with the work (for example, commercial or personal character announcements, appeals, advertisements, destructive programs, games);

- to make activity, which unnecessarily puts under load resources of Informational systems, considering other needs of Users of Informational systems (for example, unnecessarily use the Internet, to print without necessity large number of document copies, to stay opened files that are on the file server, which are not necessary for work);

- to load accessible in the Internet programs;

- independently install the software of the computer;

- unauthorized to pass copies of the software of working data to third person;

- without the coordination with the member of the board of DLV create for himself or give other Users the remote access to his work station, portative computer or resources of the server;

- independently to change the configuration of the computer, to move stationary equipment of the office and eliminate any damages of the computer equipment;

- to the system of permanent power supply of the computer connect any electronic devices, except computers, monitors and printing equipment.

The User of Informational systems has responsibility for losses, which have originated because of nonobservance of established in these conditions demands.

The Administrator of Informational systems:

- creates, modifies and liquidates identifiers (accounts) of the Informational systems User and gives appropriate rights;

- if necessary limits the file capacity of the server disk or any its catalogue, informing about that all Users of this disk or catalogue via email;

- controls that Users of Informational systems resources observe conditions of the password change, established in this conditions.

The Administrator of Informational systems is entitled to:

- in weekends or out of official labor time disconnect resources of Informational systems to make supporting works, in 3 working days informing about that Users of Informational systems;

- disconnect resources of Informational systems and suspend the system's work also in working time if an emergency has happened (if possible informing about this Users in advance via phone or email).

## 14. THE PERSONAL DATA PROTECTION VIOLATIONS' PROCEDURE

In accordance with the articles 33 and 34 of the Regulation, DLV as the Data Proprietor finds, registers, investigates, values and makes decision to notify about the happened violation of the Personal data protection to Data State Inspectorate and/or the Personal data subject.

### 1. General conditions.

1.1. About any Violation of the Personal data protection or its signs, the Employee, which has determined this, immediately informs both the proprietor of Informational resources as well as the proprietor of technical resources.
1.2. In case of the Violation, the Employee within its possibilities and authorities has an obligation to guarantee the Technical and Informational resources safety until the moment of appropriate proprietor of resources appearance.

### 2. Violations' registration, investigation and evaluation

2.1. Receiving the information from the Employee, the Data processing person, the Business Partner or any Third person about a possible Violation, a responsible person (data protection specialist) (further – the **Responsible person**) immediately does the control if the information is true. In case of the Violation suspicions, they immediately are recorded in the Violation register (appendix No.1).
2.2. The responsible person takes responsibility for the Violations register's maintenance.
2.3. After the Violations' registration, the Responsible person starts investigation, establishes the Violation kind, reasons of origin, and makes decision about the risk influence on the subject data rights.
2.4. The following Violation kinds exist:
  2.4.1. Accessibility Violation – (A)
  2.4.2. Integrity Violation – (B)
  2.4.3. Privacy Violation – (C)
2.5. In case of several Violations kinds, in the Violations register indicate all appropriate designations of the Violations.
2.6. By the influence on rights and liberty of the subject data are picked out following Influences of the Violation:
  2.6.1. The Violation does not create the risk or improbable that the risk will be created – (1)
  2.6.2. The Violation can create the risk or has created the risk – (2)
  2.6.3. The Violation creates a high risk – (3)
2.7. If there are stated several Violation kinds with the different risk Values, the action regarding the notification about the Violation is made taking into an account the highest risk Influence Value.
2.8. After the Violation Influence analysis, the notification decision about it is made in accordance with these conditions.
2.9. Additionally with the Violation Influence analysis, the consequences' elimination, made by the violation, is made in accordance with the Influence that has been made by the Violation, interrupting the Informational system's work in case of necessity.

### 3. The Data State Inspectorate notification

3.1. If there is a low-probability that the Violation can create the risk of the data subject rights and liberty (Information about low risk), the Data State Inspectorate notification is not made.
3.2. If the Violation can create risk or high risk of the data subject rights and liberty, the Data Manager immediately informs Data State Inspectorate about the data protection violation, but no later than during 72 hours from the moment when the Violation has become known.
3.3. In the Data State Inspectorate notification Data Manager indicates the following:
  3.3.1. describes the Violation character, including the data subject categories and approximate quantity;

3.3.2. the data protection specialist contact information or other contact information where it is possible to receive an additional information;
3.3.3. possible consequences of the Violation;
3.3.4. measures that Data Manager has made or plans to make that to eliminate the Violation and its negative consequences.

**4. Informing the data subject about the data protection Violation**

4.1. If Data Manager finds that the Violation can create high risk of the data subject rights and liberty, Data Manager immediately informs the data subject about it.
4.2. In the data subject notification indicates the information established in the point 3.3.
4.3. The data subject notification is not done if:
4.3.1. Data Manager has done appropriate technical and organizational protection measures, and mentioned measures are applied to the Personal Data, which has been affected by the Violation, especially such measures that make the Personal Data obscure to persons that don't have access authorities to the data;
4.3.2. Data Manager has made technical and organizational activities after the Violation that a high risk of the data subject rights and liberty has not been created;
4.3.3. If the notification needs disproportionate efforts. In this case, public notification or similar connection can be used, which with an equal efficiency informs the data subjects.
4.4. If suspicions of a criminal offence arise (Third persons etc. make data theft), the Responsible person after the consultation with Manager makes decision about State Police and Data State Inspectorate notification.