"DLV" LTD

CONDICIONES DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

Tabla de contenidos

1. OBJETIVO DE CONDICIONES Y LOS TÉRMINOS

Objetivos de estas condiciones del procesamiento y la protección de los Datos personales (en adelante – las **Condiciones**) es establecer para DLV:

- medidas de la organización y la totalidad de los medios técnicos necesarios que aseguran el procesamiento y uso honestos y legítimos de los Datos personales solo en los propósitos determinados, sus almacenamiento, reanudación, tipo de corrección y remover, asegurando la protección de los derechos de cualquiera persona física a sus Datos personales;

- las exigencias técnicas cumplimentadas y organizativas de la protección del procesamiento de los Datos personales, procesando los datos de las personas físicas y asegurando la seguridad de los Recursos de información y las Sistemas de información de DLV;

- procedimiento de la violación de la protección de los Datos personales.

Estas Condiciones desarrollaban acorde de las exigencias de la Regula.

En este documento se usan siguientes términos:

Término (abreviación)	**Definición**
Amenaza	Causas que no permiten soportar la seguridad del Sistema de información de acuerdo a las exigencias establecidas de Privacidad, Disponibilidad e Integralidad de los Recursos de información. La amenaza de la seguridad del Sistema de información son las acciones intencionadas (especiales) o las acciones haciéndose por la imprudencia o el accidente que pueden despertar el daño, el aniquilamiento o prestar la disposición de el sistema a tales personas que no son autorizadas o de detrás quienes el acceso a los Recursos de información de el sistema puede ser violado o imposible. La posibilidad de la amenaza establece la Vulnerabilidad del sistema.
Registros de auditoría	Grabaciones de la memoria del sistema de información que se creen en los estadios diferentes del procesamiento de la información para estos registros se pueden ser revistar en orden determinado posteriormente y observar el progreso del proceso examinado.
Información muy valiosa	Información, usando que no en el lugar, cambiando no sancionado, dañado o haciéndose no disponible a las personas autorizadas en alguien período del tiempo, las pérdidas substanciosas y durables pueden surgir, la reputación de DLV puede sufrir y la violación de la protección de los Datos personales puede provocados.
Autenticidad	Particularidad que identifica que la identidad del objetivo o el recurso es tal como identicaba.
Datos biométricos	Los datos personales que tienen relación con los rasgos físicos y los rasgos de comportamiento que permiten identificar únicamente esta persona, por ejemplo, las fotografías de persona o datos de las huellas dactilares.
Core HR Data	Nombre, apellido, código personal, fecha de nacimiento, sexo, fotografía (fabricación de aseguro), domicilio, teléfono, dirección de correo electrónico, número de la cuenta bancaria, asunto personal (incluyendo la información de la declaración de trabajo (CV; certificación de lengua oficial, datos de documentos de educación; revocaciones), contrato de trabajo, tarjeta de Inspección de salud obligada, aforamiento de riesgos de ambiente de trabajo en ambiente de trabajo de Empleado, función, enseñanzas, aforamiento de actividad, promociones, datos

	de conducta y disciplina), unidades de departamentos / actividad del empleador, datos de ambiente de trabajo, información de salario, información de datos de enfermedades y datos personalizados (SSI), datos de impuestos y datos de aseguramiento social, detalles de chapa de matrícula de automóviles, datos de edad de niños de Empleado (Número de acta de nacimiento de niños de Empleado y fecha de expedición para concesión de vacación adicional), datos de invalidez (para la prestación de vacación adicional), en casos particulares los Datos personales para formalización de la vacación de trabajo (copia de la aprobación a estada, los datos de pasaporte del Empleado del tercera país) o de visa, reservación de hotel, datos de la registración de las certificaciones de resoluciones/ sobre matrimonio (en caso de alteración de apellido).
Empleado	Existentes empleados (~400), ex empleados de DLV y candidatos de trabajo.
Análisis de datos	Datos se usan en tal tipo que analiza las conductas y los modelos y que permite sacar conclusiones en cado caso para mejorar la eficiencia, la capacidad competitiva y / o en ingreso.
Persona del procesamiento de Datos	Término “Persona del procesamiento de Datos” corresponde a la determinación establecida en punto 8 de artículo 4 de la Regula. La sociedad que procesa los Datos personales en nombre de Jefe de Datos. Si la sociedad almacena o procesa los Datos personales, pero no administra (no controla) los Datos personales y procesa los Datos personales que se basan acorde de las instrucciones del Jefe de Datos, entonces esta sociedad es "Persona del procesamiento de Datos". En proceso del procesamiento de datos pueden participar los representantes de servicios (por ejemplo, el proveedor de los servicios de la cuantificación de salarios, proveedor de IT servicios).
Jefe de Datos	Término “Jefe de Datos” corresponde a la determinación establecida en punto 7 de artículo 4 de la Regula. La Sociedad que toma la decisión porque y en que forma (esto es establece los objetivos y medios, por vía de que) se procesan los Datos personales. Tomando la decisión sobre quien administra los Datos personales, necesita contestar a siguientes cuestiones: - ¿quien toma la decisión que información será almacenada? - ¿quien toma la decisión a utilización la información y objetivos? - ¿quien toma la decisión a medias de procesamiento de los Datos personales? Si la sociedad administra y tiene la responsabilidad a los Datos personales (situados en su provisión) es Jefe de Datos.
DLV	“DLV” LTD – es la persona jurídica con número registral único No.40003227719, domicilio jurídico: Kridenera dambis 9, Riga, LV-1019 (DLV dependado de sitio web: www.dlvbet.lv; salas de juego de DLV: “Zilais Dimants”, “Dimats Z” y “Dimanta Bingo”) que activa en el estatuto de Jefe de los Datos personales. Lista en que se enumeran los lugares de la prestación de servicios de DLV, es disponible en el sitio web www.dlvbet.lv.
Amenazas	Cualquier acontecimiento que puede causar una pérdida de DLV. Amenazas pueden ser diferentes – catástrofes diferentes, terrorismo, pérdida de financiación de presupuesto, daños de comunicación, daños de datos, errores, actividad de empleados contraria a derecho o maliciosa (también pasividad) y otro.
Protección física	Protección de los Recursos de información contra las Amenazas que surgen de influencia física en portadores de información (por ejemplo robo, caída de tensión, daños de dispositivos y otro).
Información del acceso	Información de la circulación interior para cual jefe de los Recursos de

restringido	información establece el círculo de las personas admisibles.
Influjo	Resultado del Incidente de la seguridad de Información.
Vulnerabilidad	Imperfección del sistema de información que permite la implementación de cualquier Amenaza establecida y la influencia en la seguridad del sistema.
Incidente	Incidente en el que las Amenazas del sistema de información influyeron negativamente a actividad del sistema de información usando sus desventajas.
Recursos de información, información	Los Ficheros de datos, los bases de datos, los archivos y otra información (independientemente del tipo de portadores de información).
Jefe de recursos de información	Persona que tiene la responsabilidad de los Recursos de información (sus Accesibilidad, Integridad, Privacidad, Consecuencias de uso) y las obligaciones de que determinadas en las normativas de DLV.
Sistema (-as) de Información	Entrada, almacenamiento y procesamiento de datos en el sistema computarizada que estipulan el acceso de Consumidor a en ella datos almacenados o información, o en alguna forma la totalidad fijada las estructuradas de los Datos personales que está disponible, considerando apropiados criterios identificando de la persona.
Administrador de el sistema de información	Persona que planifica, controla y administra el uso del sistema y que tiene responsabilidad del funcionamiento de ella.
Integralidad	Caracteriza en que grado de información almacenarse y/o transmitirse completo, certero, veraz y actual.
Categorías especiales de los Datos personales	Tipos de Datos personales establecidos en artículo 9 de la Regula que revelan cualquier información sobre la persona indicada en continuación: raza o etnicidad, credos políticos, concepciones religiosas o filosóficas o participación en un sindicato. Las categorías especiales de los Datos personales se refieren también a los datos genéticos, los datos biométricos (por ejemplo, las huellas dactilares o las fotografías de la cara), los datos de salud, los datos de la vida de sexo o la inclinación sexual, y también cualquier Datos personales que se relacionan a las sentencias o el delito penal.
Clasificación	Asignación del nivel de Privacidad, Accesibilidad y Valor.
Cliente	a) cualquier persona física que usa, usaba o expresa el deseo de usar cualquieras prestamos servicios de DLV o en cualquier otro modo es conexa con ellos (incluyendo los Clientes en salas de azar, los Clientes en juegos de azar interactivos, visitantes); b) cualquier persona física que actúa de nombre de persona jurídica, proveedor u otro compañero de negocio de DLV y presta tal persona jurídica.
Confidencialidad	Característica en que la información no es disponible o no es divulgada a los individuos desautorizados, los sistemas o los procesos.
Intereses legítimos	Surgen, si procesamiento de los Datos personales es necesita en los objetivos de los Intereses legítimos de Jefe de Datos o Terceras, excepto las cosas cuando los intereses del Sujeto de los datos o los derechos libertades principales son más importantes que tal Intereses legítimos. Ejemplos de los Intereses legítimos esto es el procesamiento de los Datos personales en los objetivos exploratorios o para eliminar los delitos penales.

Consumidor	Persona jurídica o física que hizo el contrato con DLV sobre el uso de datos (incluso los Empleados) o que con fundamento en demanda recibe los datos a DLV o en el orden especificado en las reglas.
Protección lógico	Protección de los Datos o los Recursos de información que se realiza por vía de los medios de software, por ejemplo, identificando el Consumador de el sistema de información, verificando la correspondencia de su autorizamiento para actividades correspondientes de IS, protegiendo la información contra el cambiamiento o la eliminación intencionado o accidental.
Partes contratantes	Personas físicas (esto es no la sociedad) que prestan / prestaron los servicios a DLV, pero no acorde del contracto de trabajo.
Imperfección	Caracteriza el grado de la Vulnerabilidad de sistema al implementar una Amenaza específica, por ejemplo, sistema administrativa débil, obligaciones, responsabilidad no exactamente establecidas, no se realiza el control de acceso o el control es no completo (tanto acceso físico, como y acceso lógico), no están condiciones de la seguridad de el sistema de información y otros.
Datos personales	Término “Datos personales” corresponde a la definición establecida en el punto 1 de artículo 4 de la Regula. Cualquier información sobre la persona física viva que directo o indirecto permite identificar esta persona. Los Datos personales pueden incluir nombre, apellido, código personal, online-identificador, información sobre local de la persona o cualquier otra información que es característicamente para esta persona y que permite identificar la persona o hace la persona identificable. La Regula se refiere tanto a los Datos personales autorizados, como y a las sistemas manuales de registración de datos en que los Datos personales están disponibles acorde los criterios concretos. Pueden incluir las listas de registro manual disponiéndose cronológico que incluyen los Datos personales. Los Datos personales que son seudónimos – por ejemplo con ayuda de la clave los datos codificados - pueden incluir en la región de la actividad de la Regula en relación cuanto difícil conceder el seudónimo a la persona concreta.
Procesamiento de los Datos personales	Término “Procesamiento de los Datos personales” corresponde a la definición establecida en el punto 2 de artículo 4 de la Regula. Cualquier actividad o conjunto de actividades que se realizan con los Datos personales, por ejemplo, de cualquier tipo recolección de los Datos personales, uso, registración, organización, transformación, distribución, aniquilamiento, almacenamiento o cualquier otra actividad que hacen los Datos personales disponibles. Almacenamiento puede realizar o bien manualmente, o bien usando las sistemas automatizadas, por ejemplo, las sistemas de tecnologías de la información (correspondientemente se interpretando "procesar" и "procesamiento").
Violación de la protección de los Datos personales (en adelante – la Violación)	Término “Violación de protección de los Datos personales” corresponde a la definición establecida en el punto 12 de artículo 4 de la Regula. Violación de laseguridad como resultado del que pasan aniquilamiento accidental o ilegal, pérdida, transformación, divulgación prohibida o acceso a remitidos, almacenados o a otras maneras los Datos personales procesados.
Accesibilidad	Caracteriza en cual volumen las personas autorizadas pueden recibir el acceso a la información necesita a más tardar el tiempo especificado después del momento de la petición de la Información.
Perfilado	Término “Perfilado” corresponde a la definición establecida en el punto 4 de

	artículo 4 de la regula. Procesamiento autorizado de los Datos personales para estimar concretos aspectos personales conexo con la persona física, para analizar o prever productividad, decisiones, deseos, pertenencia y / o conducta de persona (y apropiadamente se interpreta "Perfil").
Regula	La Regula del Parlamento Europeo y Consejo Europeo (CE) desde el 27 de abril de 2016 № 2016/679 sobre la protección de las personas físicas en relación con el procesamiento de los Datos personales y la circulación libertada de tal datos y a causa de que se anula la Directiva № 95/46/EK (la Regula general de la protección de los datos).
Riesgo (riesgo)	La incapacidad probable de DLV realizar por completo y cualitativo de cualquiera su obligaciones o funciones. En el contexto de la seguridad de la información se examinan solo esos riesgos que conexos con el funcionamiento de las Sistemas de información.
Recursos tecnológicos	Software (realizable código de programa y ficheros de configuración que aseguran funcionamiento de el sistema de información), ordenadores, aparatos de redes de ordenador, líneas de comunicación y otros medios técnicos que usan para procesamiento, propagación y almacenamiento de información.
Administrador de los Recursos tecnológicos	Persona que tiene la responsabilidad a servició y seguridad de Recursos tecnológicos y seguridad de los Recursos tecnológicos.
Tercero	Cualquier persona o sociedad, agencia u otra organización (que no es sujeto de datos, Administrador de los Datos o Persona del Procesamiento de Datos) que en sumisión directa de Jefe de Datos o Persona del Procesamiento de Datos está autorizado procesar los Datos personales.
Valor	Importancia del Recurso de información de DLV que se determina, valorando las pérdidas posibles de cuales la pérdida, el daño o cayendo de la información en manos de las personas no autorizadas pueden surgir.
Información de valor promedio	Cuando la información se usa en un lugar incorreto, la se cambia sin autorización, la se daña o la se convierte inaccesible a las personal autorizadas por alguien tiempo, DLV puede sufrir unas pérdidas graves, la reputación de DLV puede sufrir y una violación de la protección de Datos personales puede ser provocado.
Información accesible	Información que es disponible libremente a los Empleados de DLV y cualquier otra persona que pregunto esa información.
Información de bajo riesgo	Cuando la información se usa en un lugar incorreto, se cambia sin autorización, se daña o se convierte inaccesible a las personal autorizadas por alguien tiempo, DLV no sufre unas pérdidas graves, o una violación considerabla de la actividad no se surge.

2. INFORMACIÓN GENERAL

Sujetos de datos, categorías del procesamiento de los Datos personales (también las Categorías especiales de los datos personales) y tipos, objetivos del procesamiento de los Datos personales, fuentes, base jurídica, Perfilado, propagación de los Datos personales, almacenamiento de los Datos personales, territorio geográfico del procesamiento de los Datos personales, término del almacenamiento.

Sujetos de datos:	**Empleados**	**Partes entrándose de contrato**	**Clientes**
Categorías de los Datos personales procesados, también categorías especiales de datos personales y tipos	- En relación con los Empleados apropiados de Core HR Data, la correspondencia del correo electrónico, la fotografía (video vigilancia), En relación con los Empleados, los administradores – datos de los antecedentes penales. - En relación con los Exempleados de Core HR Data (los Exempleados pueden requerir unos informes, unas características y similares), correspondencia del correo electrónico, fotografía (video vigilancia) en un volumen más pequeño, no almacenando la información sobre los datos de la enfermedad y los datos de la jubilación (SIP). - En relación con los pretendientes de trabajo: nombre, apellido, domicilio, número de teléfono, CV, referencias de los empleadores anteriores y notas de interviuar de los pretendientes de trabajo. **Categorías especiales de los Datos personales:** - **Datos de la salud** (Inspecciones de salud obligadas, y también, para realizar la investigación de los incidentes de trabajo (del hospitalario solicita tal informe médico sobre la gravedad de la salud del accidentado (Empleado)));	Nombre, apellido, código personal, dirección, número de teléfono, dirección de correo electrónico, número de IVA, contrato si la Parte cerrándose el contrato actua en el local donde DLV hace video vigilancia, también fotografía de la Parte contratarte. **Categorías especiales de los Datos personales**: no se procesan	**Datos de identificación**, por ejemplo: nombre, apellido, código personal, fecha de nacimiento, sexo, fotografía, datos de los documentos verificandos la identidad (por ejemplo: datos del pasaporte, datos del tarjeta ID). **Información de contacto**, por ejemplo: dirección del domicilio fiscal o real, número de teléfono, dirección de Correo electrónico. **Datos financieros**, por ejemplo: información de tarjeta crédito de banco del Cliente, para pagar la suma monetaria para realizar la apuesta; el número de la cuenta bancaria del Cliente en la cual la ganancia se paga. **Datos que se reciben y / o crean, cumpliendo con las obligaciones prescritas por los actos normativos**, por ejemplo: los datos que consisten en las peticiones de la información que recibidos de las instituciones de la indagación, notarios jurados, instituciones de impuestos administrativos, tribunales y jurados juduciales **Datos de las comunicaciones** que se captan cuando el Cliente visita las salas de juego y

	- Información sobre las violaciones de la infracción de las reglas del tráfico; - Participación en las organizaciones de sindicato /interrupción del contrato de sindicato del empleado (en caso de la interrupción del contrato de trabajo). En relación con los pretendientes de trabajo los Datos personales de la Categoría especial no se procesan.		los sitios web de DLV donde DLV presta los servicios o se conecta con DLV vía teléfono, en correspondencia vía Correo electrónico, avisos y otros medios de comunicación, por ejemplo: medios de comunicación social, datos que recibidos en el visite del Cliente del sítio web de DLV o se pone en contacto con DLV con ayuda de otros canales, y también **las grabaciones visuales y/o las grabaciones audio** (fotografía del Cliente por haciendo la video vigilancia). **Los datos conexos con los servicios**, por ejemplo: servicios recibidos, ganancias pagadas, solicitudes prestadas, demandas y quejas.
Objetivos de procesamiento	En los objetivos del impuesto y los objetivos del pago; para realizar las funciones de la gestión (la estrategia del negocio, los objetivos del marketing y la publicidad); - para prevenir o divulgar las actividades delictivas en conexión a la protección de la propiedad o la propiedad disponible a DLV y para defender los intereses vitales del Empleado como el sujeto de datos, incluyendo la vida y la salud; - para observar los Intereses legítimos de DLV (en los objetivos de control y mejorar la calidad del servició prestado y/o el servició de los Clientes; para valorar, estimular la productividad; para asegurar las probanzas sobre las demandas de la desconformidad de los	En los objetivos del impuesto y los objetivos del pago; para realizar las funciones de la gestión (la estrategia del negocio, los objetivos del marketing y la publicidad); - para prevenir o divulgar las actividades delictivas en conexión a la protección de la propiedad o el uso de la protección de la propiedad existente, para defender los intereses vitales de la Parte contratante como el sujeto de datos, incluyendo la vida y la salud; - para asegurar la realización de las obligaciones establecidas en la ley de DLV como Jefe de Datos y realizar las exigencias de las reglas aplicables;	**Para realizar las obligaciones jurídicas y verificar la identidad del Cliente:** para la realización las leyes y los actos normativos aplicables (incluyendo, pero no solo la obligación de DLV es la obligación verificar la edad de los visitantes de los casinos, las salas de juego y las salas de bingo, no admitir la participación de los menores de edad en los juegos de azar interactivos o en los sorteos interactivos y prevenir la participación ulterior en los juegos de azar de los jugadores dependientes de los juegos de azar interactivos (según la solicitud de la persona que ella no se admitirá en las salas de juego), también la obligación de DLV es el pago del impuesto sobre la renta

	servicios y/o la realización de las obligaciones del contrato, y también para asegurar las probanzas sobre la demanda posible que basa en el delito; - para los objetivos conexos con el sitio web de DLV (por ejemplo, indicando la información de contacto del Empleado); - para asegurar la realización de las obligaciones de DLV y la realización de las reglas DLV como Jefe de Datos establecidas en la ley; - para sancionar y controlar el acceso a los canales digitales y sus actividad, eliminar el acceso no sancionado y su uso desleal, y para asegurar la seguridad de la información en base de la realización del contrato, o para realizar la obligación jurídica o controlar la autorización de los servicios digitales de DLV, el acceso y la actividad de acuerdo al consentimiento del Empleado o los intereses legítimos de DLV; - para mejorar las sistemas técnicas, la infraestructura IT, ajustar el imagen del servicio en los equipos y desarrollar los servicios de DLV, por ejemplo: testando y mejorando las sistemas técnicas y la infraestructura IT, mejorar las sistemas técnicas y la infraestructura IT en base de los intereses legítimos de DLV; - para establecer, realizar y defender las reclamaciones: para establecer, realizar, defender y ceder las reclamaciones, o para realizar la obligación jurídica o realizar las	- para sancionar y controlar el acceso a los canales digitales y su actividad, eliminar el acceso no sancionado y su uso desleal, y asegurar la seguridad de la información en base de la realización del contrato, o para realizar las obligaciones jurídicas, o controlar la autorización a los canales digitales de DLV, el acceso y la actividad de acuerdo con el consentimiento de la Parte contratante o en los intereses legítimos de DLV; - para mejorar los sistemas técnicas, las infraestructuras IT, ajustar el equipo del imagen del servicio y el mejoramiento de los servicios de DLV, por ejemplo: testando y mejorando las sistemas técnicas y la infraestructura IT en base de los intereses legítimos de DLV mejorar las sistemas técnicas y la infraestructura IT; - para establecer, realizar y defender las reclamaciones: para establecer, realizar, defender y ceder las reclamaciones, o para realizar la obligación jurídica o realizar las reclamaciones en los intereses legítimos de DLV.	de la población por las ganancias (PNH) en el orden y el volumen establecidos en las reglas; también la obligación de DLV es el pago de la ganancia al jugador en el orden establecido en las reglas (tercera parte de artículo 36 de la Ley sobre Juegos de azar y sorteos); también la obligación de DLV es la realización de los estudios de los Clientes en el orden establecido en las reglas, para proveer la información a las instituciones competentes, para prevenir, divulgar, investigar e informar sobre la legalización probable de los fondos resultantes del delito, la financiación del terrorismo, si el Cliente acata las sanciones financieras y es la persona políticamente importante), o para los intereses legítimos de DLV aseguran la gestión bien reflexionado de los riesgos y la administración de la empresa **Para la gestión general de las relaciones de los Clientes y el aseguramiento de los servicios de acceso y la administración:** para la prestación de servicio, para el aseguramiento de la actualidad de datos y su corrección, verificando y complementando los datos, usando los fuentes exteriores y interiores en base de la realización de servicio o para la realización de las obligaciones jurídicos. **Para la protección de intereses del Cliente y/o DLV:** para la protección

	reclamaciones en los intereses legítimos de DLV.		de los intereses del Cliente y/o DLV y servició de calidad de los servicios prestados de DLV y, para prestar las pruebas, en base de la realización del servicio o, para realizar las obligaciones jurídicos o consentimiento del Cliente, o en los intereses legítimos de DLV eliminar, limitar y investigar el uso desleal o ilegal de los productos y servicios de DLV o la creación de los impedimentos en ellos, para la educación interior o el aseguramiento de los servicios de calidad. Para la garantía de la seguridad de DLV y/o del Cliente, la protección de la vida y salud del Cliente y otros derechos de DLV el Cliente, en base de los intereses legítimos de DLV defender sus Clientes y los activos de los Clientes y DLV. **Para la eliminación del uso desleal de los servicios y el aseguramiento de la correspondencia de servicios**: para el seccionamiento y el control del acceso a los canales digitales y su actividad, la eliminación del acceso no sancionado y su uso desleal, y para el aseguramiento de la seguridad de información, en base de la realización del contrato o para la realización de las obligaciones jurídicos o acorde de consentimiento del Cliente o en los interese legítimos de DLV controlar la autorización, el acceso y la actividad de los servicios digitales de DLV.

			Para el mejoramiento de el sistema técnica, la infraestructura IT, el ajustamiento de los equipos de la imagen de servicio y el desarrollo de os servicios de DLV, por ejemplo: testando y mejorando los sistemas técnicas y la infraestructura IT, en base de los intereses legítimos de DLV mejorar las sistemas técnicas y la infraestructura IT. **Para el establecimiento, la realización y la protección de las reclamaciones:** para el establecimiento, la realización, la protección y para ceder las reclamaciones, o, para la realización de las obligaciones jurídicas, o en los intereses legítimos de DLV realizar las reclamaciones.
Fuentes	Los Datos personales del Empleado pueden recogerse precisamente del Empleado, de las relaciones del contrato de trabajo, y también de las fuentes exteriores, por ejemplo, las agencias de empleo, las empresas del alistamiento de los empleados, los portales de representaciones de trabajo, SIP, de los registros públicos y la información disponible público.	Los Datos personales de la Parte contratarte pueden recogerse precisamente de la Parte contratarte, de las relaciones del contrato de trabajo, y también de las fuentes exteriores, por ejemplo, de los registros públicos y la información disponible público.	Los Datos personales del Cliente pueden recogerse precisamente del Cliente, de las fuentes exteriores y las fuentes de uso del Cliente, por ejemplo, de los registros públicos y la información disponible público.
Base jurídica	- Para contratar y realizar el contrato de trabajo; - Para realizar las obligaciones jurídicas de DLV de acuerdo a las exigencias de los reglamentos que establecen las obligaciones del empresario en conexión con los Empleados (la Ley de trabajo, la regla de	- Para realizar el contrato; - Para realizar las obligaciones jurídicas de DLV de acuerdo a las exigencias de los reglamentos (las leyes, que establecen la regulación de la contabilidad y otro); - Para el aseguramiento de los	- Para realizar el contrato (servicio); - Para realizar las obligaciones jurídicas de DLV de acuerdo a las peticiones de los reglamentos de los Juegos de azar y sorteos (la Ley de recursos jumanos acerca de los Juegos de azar y los sorteos y la Regla de

	Gabinete de Ministros Nr.950 de 25 de agosto de 2009 “La Investigación de los accidentes en trabajo y el orden de registro”, las leyes que establecen el seguro social estatal, el ordenamiento de la contabilidad y otro); - para el aseguramiento de los intereses legítimos de DLV; - acorde de consentimiento del Empleado.	intereses legítimos de DLV; - Según del consentimiento de la Parte contratarte.	Gabinete de Ministros № 715 “La regla de la verificación y la registración de la identidad de jugadores de los Juegos de azar y los sorteos interactivos”), en la Ley de la protección de los derechos de consumidores, la Prevención de la Legalización de los fondos resultantes del delito y la Financiación del terrorismo, en la Ley “Sobre la contabilidad”, en la Ley “Sobre impuesto a la renta de la población”, en la Ley “Sobre los impuestos y tasas”, en la Ley “Sobre impuesta y la tasa de los sorteos y los juegos de azar”, en la Ley sobre el archivo y otros reglamentos de la República de Letonia; - Para la aseguración de los Intereses legítimos de DLV; - Acorde del consentimiento del Cliente.
El Perfilado, las propuestas personalizadas y la toma automatizada de las decisiones	No realizado	No realizado	Para valorar los rasgos personales determinados del Cliente, para el análisis de los Datos del Cliente y la consultación en los objetivos del marketing directo, para toma automatizada de decisiones, por ejemplo: para la gestión de los riesgos, para el aseguro de la prestación de servicios remotos, incluyendo para la vigilancia de servicios, para prevenir el fraude, y esto basarse en los intereses legítimos de DLV, la realización de las obligaciones jurídicos, la realización de servicios (contrato) o el consentimiento del

			Cliente. Para el mejoramiento de la experiencia del uso de los servicios digitales del Cliente, por ejemplo, adaptando el ajustar el imagen de servicio en el equipo usando y, para preparar al Cliente las propuestas apropiadas. Si solo el Cliente no limitó el marketing directo a su mismo, DLV puede realizar el procesamiento de los Datos personales para la preparación las propuestas generales y personalizadas de DLV. Tal marketing puede ser basarse en los servicios, usados del cliente y como el Cliente usa los servicios y como el Cliente acta en los canales digitales de DLV. El perfilado, basándose en las propuestas personalizadas y marketing, cual realizarse acorde de los intereses legítimos de DLV, DLV asegura, que los Clientes pueden tomar la decisión usar el instrumento cómodo para la gestión su ajustes de privacidad. DLV puede también recoger los datos estadísticos sobre el Cliente, incluyendo sobre el comportamiento caracterizado o la manera de vivir, en base de los datos demográficos agrícolas. Los datos estadísticos para la organización del segmento/perfil pueden ser recibidos también de las fuentes exteriores y pueden ser combinados con los datos interiores de DLV.
Divulgación de los datos personales	Los Datos personales del Empleado se divulgan a: - los proveedores de	Los Datos personales de la Parte contratante se divulgan a:	Los Datos personales del cliente se divulgan a: - los proveedores

	servidores; - cualquier auditor, consultor financiero, colector de deudas, jurisconsulto, abogado jurado, notario jurado y/o jurado judicial u otra persona autorizada de DLV de procesamiento de los Datos personales a opción de DLV; - el especialista competente para valorar los Riesgos del medio de trabajo, porque necesita valorar cada lugar de trabajo del Empleado; - los prestadores de servicios sobre educación de los Empleados (en el ámbito de la seguridad contra incendios y similares); - Inspección de la supervisión de los sorteos y los juegos de azar, Servicio de Ingresos Públicos y otras instituciones (por ejemplo, agencias policiales и instituciones de investigaciones financieros, tribunales, instituciones extrajudicial de resolución de disputas, administradores del proceso de bancarrota e insolvencia); - otras personas que conexas con los servicios prestados por DLV, incluyendo los prestadores de servicios de archivo, correo y similares.	- los proveedores de servidores y otros terceros que son conexos con DLV en la prestación de servicios; - cualquier auditor, el consultor financiero, colector de deudas, jurisconsulto, abogado jurado, notario jurado y/o jurado judicial u otra persona autorizada de DLV de procesamiento de los Datos personales a opción de DLV; - Inspección de la supervisión de los sorteos y los juegos de azar, Servicio de Ingresos Públicos y otras instituciones (por ejemplo, agencias policiales e instituciones de investigaciones financieros, tribunales, instituciones extrajudicial de resolución de disputas, administradores del proceso de bancarrota e insolvencia); - Otras personas que conexas con los servicios prestados por DLV, incluyendo los prestadores de los servicios de archivo, correo y similares.	de servidores y otros terceros que son conexos con DLV en la prestación de servicios; - cualquier auditor, el consultor financiero, colector de deudas, jurisconsulto, abogado jurado, notario jurado y/o jurado judicial u otra persona autorizada de DLV de procesamiento de los Datos personales a opción de DLV; - Inspección de la supervisión de los sorteos y los juegos de azar, Servicio de Ingresos Públicos y otras instituciones (por ejemplo, agencias policiales e instituciones de investigaciones financieros, tribunales, instituciones extrajudicial de resolución de disputas, administradores del proceso de bancarrota e insolvencia); - Las empresas reconocidas de análisis de mercado y estudio de la opinión pública (en el contexto de CE) – la realización de sondeos y exploraciones conexos con los servicios propinados de DLV; - otras personas que conexos con los servicios prestados por DLV, incluyendo los prestadores de los servicios de archivo, correo y similares.
Almacenamiento de los Datos personales	Los contratos de trabajo, la descripción de trabajo, las condiciones del orden de trabajo, las instrucciones, otros documentos (el certificado de la lengua oficial, el permiso de residencia) se almacenan en formato de papel en la oficina, en las carpetas, en	Los Contratos firmados por las partes se almacenan por escrito en la oficina en el armario cerrado.	Los contratos del Cliente, los cuestionarios complementados (la solicitud de la Programa de lealtad) en el formo físico se almacenan en las carpetas (en las unidades estructurales), hay en el armario. Información del Cliente

	el armario cerrado. Los contratos de trabajo ejecutados en el formato electrónico se almacenan en el ordenador y en el servidor en la carpeta compartimentada “Servicio jurídico”. Registros de contabilidad de los contratos de trabajo a los años anteriores es disponibles tanto por escrito (en el ordenador y en el servidor) como y en formato de papel (en la oficina, en las carpetas, en el armario cerrado). Las tarjetas de las verificaciones de salud obligatorias de los empleados se almacenan en la oficina – en la carpeta, en el armario cerrado. Las copias de los contratos de trabajo se almacenan en los objetos (en unas carpetas, en un armario cerrado) – para la prestación inmediata a Inspección de trabajo estatal durante las verificaciones (verificaciones en relación con la colocación laboral ilegal). Unas normativas sobre el movimiento de los Empleados – tanto por electrónico (en un ordenador en un servidor) como y por escrito (en una oficina, en un armario cerrado) hace la sección de personal, se transfieren para el tratamiento en el departamento de contabilidad. Las cuentas bancarias de los Empleados se transfieren en el departamento de contabilidad por escrito para pagar el salario. Los órdenes de contabilidad se almacenan en el departamento de contabilidad (en las		se almacena en el sistema de gestión de los clientes.

	carpetas, en un armario cerrado). Con los datos personales de los Empleados (los pretendientes de trabajo) puede familiarizarse la administración de DLV o su Empleado autorizado (incluyendo el prestador de la externalización de la contabilidad financiera y otro) en los objetivos necesarios. Nombres y apellidos de los Empleados pueden ser divulgados a otro Empleados y Clientes de DLV, pero DLV puede divulgar otros Datos personales solo si el consentimiento del Empleado o el pretendiente apropiado ha recibido.		
Región geográfica de procesamiento	Los Datos personales se procesan en zona de Unión Europea/Espacio Económico Europeo (CE/EEE).		
Período del almacenamiento	Período del almacenamiento de los Datos personales procesados puede ser fundamentarse del contracto, los intereses legítimos de DLV o los actos normativos aplicables (por ejemplo: las leyes sobre contabilidad, archivos, legalización de los fondos resultanes del delito, limitaciones, derechos civiles y otros). DLV almacena los Datos personales de acuerdo a los objetivos e las intenciones de los Datos personales como y de acuerdo a las exigencias de las Regulas y los actos normativos, incluyendo para la observación de los Intereses legítimos de DLV (para asegurar de las probanzas sobre las demandas de la disconformidad de los servicios y/o incumplimiento de las obligaciones del contracto, y también para asegurar de las pruebas contra las demandas posibles que parten del delito), DLV almacena los Datos personales durante diez años del día de la realización del servicio o el contracto. Después de fin del período del almacenamiento DLV borra los ficheros que incluidan los Datos personales.		

3. RECURSOS DE INFORMACIÓN, RECURSOS TÉCNICOS Y PERSONAS RESPONSABLES DE LA PROTECCIÓN DE LOS DATOS PERSONALES, SUS DERECHOS Y OBLIGACIONES

Administración de los recursos de información y los recursos técnicos:

En general la gestión de DLV es responsable para la protección, la seguridad de la información y el proceso de la optimización de los Datos personales que independientemente o con ayuda de la persona nominada controla la confiabilidad del sistema del procesamiento de los Datos personales.

La gestión nomina la especialista/-as del procesamiento de los Datos personales y/o la persona/-as de soporte de los Recursos de información y los recursos técnicos, o tiene la obligación realizar los cometidos apropiados mismo.

La gestión o la especialista del procesamiento de los Datos personales o la persona de soporte de los Recursos de información y los recursos técnicos nomina las personas que están subordinados de la especialista del procesamiento de los Datos personales o la persona de soporte de los Recursos de información o los recursos técnicos y que se hace responsable a la seguridad de las Sistemas de información.

La gestión en el marco del presupuesto asegura las personas de soporte de los Recursos de información y los recursos técnicos con las medias que son necesitas para las medidas de la seguridad de las Sistemas de información.

Persona de soporte de los recursos de información:

- en común de las personas de soporte de los recursos técnicos y (si es posible) con el representante de la información realiza el análisis de los riesgos conexos con los Recursos de información;
- asegura las medidas de la Protección lógico;
- asegura el Control de auditoría de las Sistemas de información, y también su mantenimiento y Accesibilidad para la verificación, a causa de las condiciones de la seguridad de las Sistemas de información;
- establece el orden en el cual los Consumidores de las Sistemas de información se conceden los derechos del acceso a los Recursos de información y las actividades con ellos, y organiza el control del uso de estos recursos;
- asegura la fabricación y el almacenamiento de las copias de respaldo de los Recursos de información, y también la reanudación de los Recursos de información, si el funcionamiento de las Sistemas de información fue interrumpido o imposible debido a los daños de los recursos técnicos u otras causas.

Persona de soporte de los recursos técnicos:

- Asegura las medidas de la protección física;
- Participa en el análisis de los riesgos, establece con los recursos técnicos conexas Amenazas de las Sistemas de información y valora la probabilidad de la realización de estas Amenazas;
- asegura la reanudación de los recursos técnicos, si tales están dañados;
- asegura la reanudación de los recursos técnicos;

Persona de soporte de los Recursos de información y los recursos técnicos establece las obligaciones de los Empleados en el ámbito de la seguridad de las Sistemas de información y asegura la educación de los Empleados y la verificación de conocimiento en el ámbito de la protección de los Recursos de información y los recursos técnicos.

4. CLASIFICACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES DE ACUERDO AL GRADO DEL VALOR Y LA CONFIDENCIALIDAD

Objetivo de la clasificación de la información identificar toda importancia de la información a la disposición de DLV y asegura la protección de cualquiera grupa de la información de acuerdo a su nivel de clasificación.

Personas de soporte de los Recursos de información realizan la Clasificación de los Recursos de información al grado de Valor, Confidencialidad y Accesibilidad. Clasificación de la información se realiza a causa de la demanda de la persona de soporte de los Recurso de información, si tal establece.

Clasificación de la información se refiere de toda información con la independencia del portador de información (papel, microfilmes, videocasetes, cintas magnéticas, casetes, compact disk, disco rígido de ordenadores, disquetes u otros portadores de información).

Información se clasifica al Grado de la confidencialidad, al evaluar de las Amenazas de su pérdida desautorizada, de la manera siguiente:

- Información accesible;
- Información del acceso restringido.

Información se clasifica al Grado del valor al evaluar de las Amenazas de la Integridad de la información, de la manera siguiente:

- Información de gran valor;
- Información valiosa promedio.

Información por el Nivel de la accesibilidad al valorar de las Amenazas de su Accesibilidad. Clasificando, establece también tiempo admisible a cual los Recursos de información pueden ser no disponibles. Se clasifican al siguiente modo:

- Información disponible permanentemente;
- Información disponible solo en horas de trabajo.

Información que no clasificada de acuerdo a los Principios de la confidencialidad, automáticamente se considera como la Información del acceso restringido.

Si en un portador de información la informacion se almacena que se clasificada con los niveles diferentes, el más alto nivel de la información que existe en esto portador se indica como el nivel general de la clasificación del portador de información.

Todos los portadores de información del Acceso restringido debe ser siguiente marca sobre la clasificación de la información.

5. RECURSOS TÉCNICOS CON CUALES SE ASEGURA EL TRATAMIENTO DE DATOS PERSONALES

Procesamiento de los Datos personales se asegura con siguientes recursos técnicos:

- las estaciones de trabajo estacionarias, portátiles o los ordenadores personales;
- servidores;
- sistemas de vigilancia;
- otros equipos y el software por necesidad.

6. PROCEDIMIENTO DE LA ORGANIZACIÓN DEL TRATAMIENTO DE LOS DATOS PERSONALES

Procesamiento de los Datos personales se produce en los locales de DLV, en los locales donde se sitúan los servidores de DLV, y en cualquier lugar de cual se asegura el acceso alejado a los Recursos de información. Los Datos personales se procesan constantemente o por necesidad, de acuerdo a los objetivos de su procesamiento.

DLV procesa los Datos personales de acuerdo a lo establecido en los actos normativos y solo entonces, si es a lo menos uno de siguientes condiciones:

- Consentimiento del sujeto de los Datos personales es recibido;

- Procesamiento de los Datos personales consiste en las obligaciones del contrato del sujeto de datos o a lacondición de la petición del sujeto de datos, el procesamiento de los Datos personales es necesita para concluir siguiente contrato;

- procesamiento de los Datos personales es necesita DLV para la realización de las obligaciones establecidas en la ley;

- procesamiento de los Datos personales es necesita para defender los intereses vitales del sujeto de datos, incluyendo la vida y la salud;

- procesamiento de los Datos personales es necesita para asegurar el cumplimiento de los intereses de DLV o realizar unos cometidos de poder del Estado para la realización de cuales los Datos personales se divulgan a DLV;

- procesamiento de los Datos personales es necesita, observando los derechos principales y libertad de sujeto de datos, para realizar los intereses legítimos de DLV o Tercero a quien se divulgaron los Datos personales.

7. SISTEMA DE VIGILANCIA

DLV produce video vigilancia para la prevención de unos delitos o para la divulgación conecto con la protección de la propiedad e los intereses vitales de las personas, incluyendo la protección de la vida y la salud, y también para la realización de las obligaciones establecidas en los actos normativos de los sorteos y los juegos de azar.

Video vigilancia se produce permanentemente dentro y fuera de las salas de juego de DLV.

Videos se graban a los portadores de información del ordenador que están en cada sala de juego.

Acceso a los vídeos es solo centralizado desde la oficina de DLV, conectando alejado a cado ordenador de la sala de juego.

Los vídeos se almacenan no menos de 7 días desde el momento cuando las grabaciones han creado y por el tiempo que un volumen de un portador de datos de cada sistema concreta de video vigilancia permite. Cuando el volumen de un portador de datos del sistema vídeo vigilancia se termina, los datos posteriores de la vídeo vigilancia se graban en cambio los anteriores en el portador de datos mismo.

En el contexto del obrado disciplinario, administrativo o criminal, DLV guarda el video grabación apropiada por el tiempo cuanto el obrado apropiado no termine.

Video vigilancia no es permitida en el baño y en los locales/zonas de descansar de los Empleados.

En cada sala de juego en el lugar visible por escrito necesario situar la la notificación/la pegatina que informe que está haciendo la video vigilancia, indicando en ella el objetivo de la video vigilancia, la empresa de DLV y la información de contacto.

8. DERECHOS DEL SUJETO DE DATOS (EMPLEADO, PARTE CONTRATANTE, CLIENTE)

Antes del procesamiento de los Datos personales, DLV concede la información sobre el procesamiento de los Datos personales:

- al Empleado, firmado siguiente anexo al contrato de trabajo sobre el procesamiento de los Datos personales;

- a la Parte contratante, incluido en el contrato las condiciones sobre el procesamiento de los Datos personales;

- al Cliente, poniendo al tanto el Cliente de la Solicitud sobre la confidencialidad y Política de confidencialidad.

Sujeto de datos tiene siguientes derechos:

1.1. solicitar la corrección de sus Datos personales si los no apropiados, incompletos o inexactos;

1.2. estar en contra del tratamiento de sus Datos personales, si el uso de los Datos personales se basa en los intereses legítimos, incluyendo las intenciones del perfilado de marketing directo (por ejemplo, para el recibo de las presupuestas de marketing o la participación en los sondeos);

1.3. solicitar borrar de sus Datos personales, por ejemplo, si los Datos personales se procesan en base del consentimiento, si el sujeto de datos ha retirado su consentimiento. Tal derechos no tienen vigencia, si los Datos personales, cuyos eliminación solicitado, se procesan también en base de otros bases jurídicas, por ejemplo, contratos o las obligaciones consiguiente a los actos normativos apropiados (por ejemplo, la Ley de recursos humanos sobre la prevención de la legalización de los fondos resultantes del delito y la Financiación del terrorismo) o en otros casos establecidos en la Regula;

1.4. limitar el tratamiento de sus Datos personales en conexión con las actas normativas aplicadas, por ejemplo, durante el tiempo cuando DLV valora si el sujeto de datos tiene los derechos de la eliminación sus datos;

1.5. recibir la información, si DLV procesa sus Datos personales y, si procesa, recibir el acceso a ellos y recibir la información como se procesan y a quien se transmiten;

1.6. recibir sus Datos personales que ha prestado y que se procesan en base de la realización del convenio o contrato por escrito o por cualquier formato electrónico y, si posible, transferir tales datos a otros representantes de servicios (la portabilidad de datos);

1.7. retirar su consentimiento al procesamiento de sus Datos personales, si los Datos personales se presentan a DLV en base del consentimiento del sujeto de datos;

1.8. no estar sujeto a la toma de decisiones automatizada por completo, incluyendo al perfilado, si tal toma de decisión tiene los efectos jurídicos o que asimismo visiblemente influye al sujeto de datos. ales derechos no tienen la vigencia, si la toma de decisión necesario, para hacer o realizar un contrato con el sujeto de datos, si la toma de decisión permitido acorde las actas normativas aplicables o, si el sujeto de datos da su consentimiento explícito;

1.9. presentar la apelación sobre el uso de los Datos personales por Inspección de datos estatal (www.dvi.gov.lv), si el sujeto de datos considera que el procesamiento de su Datos personales viola sus derechos e intereses en conexión con los actos normativos aplicables.

Derechos que la persona <u>NO PUEDE</u> usar (con “X” se marca los derechos que la persona física (sujeto de datos) NO PUEDE usar. Las células SIN “X” son los derechos que la persona física (sujeto de datos) PUEDE usar):

El base del procesamiento de los Datos personales:	Derechos de la eliminación de datos	Derechos de la transferencia de datos	Derechos de la objeción
Consentimiento			X pero los derechos a revocar el consentimiento
Contrato			X
Obligación legítima	X	X	X
Intereses principales		X	X
En el tarea de las	X	X	

instituciones estatales			
Intereses legítimos		X	

9. Orden en cual DLV asegura a Sujeto de datos los derechos garantizados y medidas de la seguridad de Datos personales

El seguro de los derechos del sujeto de datos.

Las demandas del Sujeto de datos:

Si es recibe la solicitud del sujeto de datos sobre de revelar o divulgar los Datos personales del sujeto se datos, disponibles para DLV, tal solicitudes examina miembro de la junta de DLV o su persona designada, y siguientes Datos personales pueden revelados o divulgados solo miembro de la junta de DLV o su persona designada, si tal divulgación o transferencia están fundadas.

Para defender los Datos personales contra la divulgación ilegal, DLV, recibiendo la demanda del sujeto de datos sobre la concesión de datos o sobre la realización de otros derechos del sujeto de datos, se cerciora en la personalidad del sujeto de datos. Para esto objetivo DLV tiene el derechos pedir del sujeto de datos indicar los Datos personales, comparando, si los datos indicados del sujeto de datos coinciden con los Datos personales apropiados disponibles para DLV. Realizando esta verificación, DLV también puede enviar el aviso de verificación al teléfono y el correo electrónico indicado del sujeto de datos (los mensajes o correos electrónicos), con la petición realizar la autorización. Si el procedimiento de verificación es fallido (por ejemplo, los datos indicados del sujeto de datos no coincide con los Datos personales, disponibles para DLV, o el sujeto de datos no realizó la autorización al mensaje o el aviso de correo electrónico enviados), DLV estará obligada a creer que el sujeto de datos no es el sujeto de los Datos personales pedidos y estará obligada a negar la demanda presentada apropiada.

Recibiendo la demanda del sujeto de datos por la realización cualquier derechos de sujeto de datos y realizando acertado el procedimiento de verificación anteriormente mencionado, DLV tiene la obligación sin tardar, con todo en cualquier caso a más tardar durante un mes de recibiendo de la demanda del sujeto de datos y del fin del procedimiento de verificación, prestar al sujeto de datos la información sobre las actividades que DLV realizó de acuerdo a la demanda presentada por el sujeto de datos. Teniendo en la cuenta la complicación de la demanda y la cantidad, DLV tiene el derecho a la prolongación del periodo de un mes a los dos meses, informando sobre esto el sujeto de datos antes el fin de primero mes e indicando la causa de tal prolongación. Si la demanda del sujeto de datos enviada con ayuda de los medios electrónicos, DLV da la respuesta también con ayuda de los medios electrónicos, excepto casos cuando esto no será posible (por ejemplo, por gran cantidad de datos) o si el sujeto de datos solicitó responder en otro modo.

DLV tiene el derecho abstenerse satisfacer la demanda del sujeto de datos con la respuesta motivada, si las circunstancias establecidas en las reglas estarán constatadas o será imposible asegurarse en la identidad del sujeto de datos, informando sobre esto el sujeto de datos por escrito. Si las demandas del sujeto de datos no son sin fundamento evidentemente o excesivos, en particular debido a su repetición regular, DLV como el Guardián de Datos puede sea: a) requerir el pago razonable, teniendo en cuenta los gastos administrativos que conexos con el aseguramiento de información o la comunicación o la realización de las actividades requeridas; sea b) negarse realizar la demanda.

Las demandas de terceros:

Si la demanda de prestar o divulgar los Datos personales disponibles para DLV se recibió de instituciones estatales o de autogestión o Terceros que no son los Empleados, la Parte contratante, o los Clientes, tal requisitos examina el miembro de la junta de DLV o su persona digitada, y los Datos personales apropiados puede presentar o revelar solo el miembro de la junta de DLV o su persona digitada, si tal divulgación o transferencia están fundadas.

En cualquier caso, si el Empleado de DLV no sabe como actuar – puede o no puede revelar alguna información – el Empleado es necesito consultarse con el miembro de la junta de DLV o con su persona digitada, y el Empleado puede actuar en apropiado caso solo como el miembro de la junta de DLV o su persona digitada ha indicado.

DLV, entregando los Datos personales, asegura la conservación de la información sobre:

- El tiempo de la transmisión de los Datos personales;
- Persona que entregó los Datos personales;
- Persona que recibió los Datos personales;
- Los Datos personales que fueron entregados.

Las Medidas de la seguridad de los Datos personales.

Para defender los Datos personales contra el acceso no sancionado, la pérdida accidental, el aniquilamiento o el daño, DLV usa las medidas de la seguridad física: los archivadores cerrados que incluyen los Datos personales; cerrados oficinas / locales con los Datos personales.

DLV usa los medios de seguridad, para asegurar la protección de los equipos y / o los ficheros contra el acceso no autorizado, la pérdida accidental, el aniquilamiento o el daño: la autorización, el archivo, la encriptación, el acceso de los Usuarios, la reglamentación de los actividades, certificados de SSL, cortafuegos.

DLV usa otras medidas de la seguridad, para defender los Datos personales contra el acceso no autorizado, la pérdida accidental, el aniquilamiento o el daño: los derechos del acceso restringido a los Datos personales (basarse en necesidad de saber); el aniquilamiento seguro de los desechos de la documentación de la información confidencial (tanto por escrito, como y electrónico), educación de los empleados.

Al procesar los Datos personales en el sistema de información, asegurarse solo el acceso de las personas autorizadas a los Datos personales, los medios técnicos y los documentos.

El administrador de las Sistemas de información en la colaboración con la persona de soporte de los Recursos tecnológicos tiene el derecho realizar las auditorías de las actividades de los Usuarios. Tales auditorías pueden incluir la realización de la auditoría de las actividades del Usuario (incluyendo de los recursos de internet concurridos), el análisis y el requerimiento de la información adicional sobre las actividades realizadas.

En el contexto de la vigilancia del uso de las Sistemas de información:

- La persona de soporte de los Recursos tecnológicos asegura que las registraciones de la Auditoría se forman sobre las Sistemas de información, cuales incluye los Recursos de información clasificados y sobre las actividades en la red de ordenador, en el cual hay el acceso a las Sistemas de información, cuales incluyen los Recursos de información clasificados. Las registraciones de la Auditoría se incluyen todos fechas y tiempo de los casos acertados y fallados de la conexión, y también el código del Usuario (incluyendo la persona de soporte de los Recursos técnicos) u otros medios de la autenticación;

- La persona de soporte de los Recursos tecnológicos asegura la integralidad de la registraciones de la Auditoría y regularmente hace las registraciones de las copias de reservo de los datos de la Auditoría de acuerdo a las reglas de estos condiciones;

- La persona de soporte de los Recursos tecnológicos regularmente controla toda actividad de los Sistemas de información, pero presta atención especial al control de la actividad de los Sistemas de información, cuales incluyen los Recursos de información clasificados. Para esto objetivo la persona de soporte de los Recursos tecnológicos a opción de su usa los programas especiales del control o los sistemas de ordenador, constatados la invasión.

La persona de soporte de los Recursos tecnológicos controla a lo menos siguientes casos:

- la reconexión fallida a el sistema de información;

- los intentos de conectarse a los Recursos de información, a cuales el Usuario no autorizado conectarse; el uso de las Sistemas de información en el tiempo inusual, por ejemplo, afuera de las ahoras de trabajo;

- los intentos duplicados del uso de los códigos del Usuario que ya fueron rechazados;
- la apropiación y el uso de los códigos del Usuario privilegiados;
- la transformación no sancionada de las configuraciones del software y la instalación inadmisible del software.

El control de los virus de los Recursos de el sistema de información:

- la persona de soporte de los Recursos tecnológicos establece el orden y realiza las medidas para la prevención de los virus en el ordenador de las Sistemas de información;
- para la prevención de los virus usa el software expresamente proporcionado para esto objetivo. Los ficheros, determinados como de virus, se renuevan inmediatamente una vez es desarrollador propone los ficheros para la reanudación;
- la persona de soporte de los Recursos tecnológicos regularmente realiza el control de las programas de antivirus, para asegurarse en su funcionalidad y encontrar nuevos ficheros, determinados como de virus.

Protección de los ordenadores personales y portátiles:

- El Propietario de la información establece que información se puede almacenar en el ordenador personal o portátil (en adelante en el texto – **los ordenadores personales**). En los ordenadores personales que se usan fuera de los locales de trabajo de DLV, almacena solo esa información que es necesita al Usuario establecido del ordenador en el tiempo establecido;
- En el ordenador personal instalan y usan solo eso software y con esa configuración, cual la persona de soporte de la Información de tecnología determinó. La funcionabilidad del ordenador personal limita al nivel de funciones necesitas para las necesidades de trabajo;

Abandonando el ordenador personal sin la vigilancia del Usuario, desconecta usando la salvapantalla con el clave, la función especial de desconexión u otro método, cual admite continuar el trabajo con el ordenador personal solo si realizaba la autentificación del Usuario;

- persona de soporte de los Recursos tecnológicos establece el orden, en cual los Empleados para las necesidades de trabajo usan sus ordenadores y usan los ordenadores de DLV fuera de locales de trabajo. Tal orden no se puede reducir en el nivel de la protección de los Recursos de información establecidos.

Protección de la red de ordenador:

- la persona de soporte de los Recursos tecnológicos elabora y mantiene el esquema de la red de ordenador en el cual se indican los equipos conectados en la red de ordenador y los servicios prestados;
- el corriente de datos entre de la red de ordenador local y la red de ordenador exterior autoriza solo esos servicios que necesarios para la realización de los funciones de DLV, para esto objetivo usa las sistemas de cortafuego;
- la persona de soporte de los Recursos tecnológicos verifica regularmente la existencia de toda conjunción exterior y se convence que hay solo esos conjunciones que corresponden a las condiciones de trabajo de DLV y que las conjunciones reservas trabajan;
- la conexión a las Sistemas de información del lugar alejado lógico defienden, usando los medios de criptografía junto el clave del Usuario tal, para determinar con seguridad la Autenticidad del Usuario.

DLV por necesidad realiza las medidas adicionales de la Protección lógica, en relación al nivel de clasificación de los recursos del sistema de información.

DLV realiza las medidas iguales de la Protección lógico para los Recursos de información, clasificados con independencia del tipo de almacenamiento de datos (incluyendo disquetes, documentos papeles, casetes de audio y otros).

DLV en colaboración con los representantes exteriores de los servicios de tecnologías de información:

- establecen las demandas de la responsabilidad de las personas incorporadas, apropiación de las cuentas temporales de los Usuarios, la administración de los cambios u otras demandas de

seguridad de las Sistemas de información;

- ordinando con los propietarios de información, se apropia los derechos de acceso a los recursos de las Sistemas de información a los representantes exteriores de las tecnologías de información solo en el volumen que es necesario para la realización de las obligaciones;
- establecen las limitaciones de la distribución de la información.

Si DLV toma la decisión confiar al representante exterior de servicios el servició de las Sistemas de información, debe asegurar el nivel de la seguridad de las Sistemas de información que es no más bajo de establecido en estas condiciones. DLV debería familiarizar el representante de los servicios exteriores con las exigencias establecidas de la seguridad de las Sistemas de información en estas condiciones. Orden de procesamiento de los Datos personales y los niveles de acceso establece la repartición de roles de los Usuarios de las Sistemas de información.

10. ESTRUCTURA DE LA CLAVE, ORDEN DE SU USO Y ACCESO

A cada Usuario de los recursos de información se apropia nombre(s) de usuario(s) (identificador(es)) del sistema de información y la clave, y también los derechos establecidos de acceso. El Usuario de el sistema de información tiene la responsabilidad a uso, conservación y no distribución del nombre de acceso asignado (identificador) y clave.

Derechos del acceso confirma el propietario apropiado de los Recursos de información. En base de la demanda del propietario de los Recursos de información, el administrador de las Sistemas de información da el acceso al Usuario a todas las Sistemas de información determinadas en la afirmación.

El Propietario de los Recursos de información debe informar el administrador de las Sistemas de información sobre esos Empleados que interrumpen las relaciones de trabajo con DLV. El Propietario de los Recursos tecnológicos después de recibo de esta información, inmediatamente anula todos derechos de acceso del Empleado apropiado de DLV a los recursos de las Sistemas de información.

El Usuario del sistema de información tiene la responsabilidad de las actividades que realizarse, usando su nombre de usuario (identificador). Autenticidad del Usuario del sistema de información establece para asegurarse que el usuario del nombre de usuario (identificador) es su propietario autorizado. Para establecimiento de la Autenticidad se usan las claves. Después de entrada del nombre de usuario (identificador) y la clave, el Usuario del sistema de información puede usar los recursos del sistema de información de acuerdo a los derechos de acceso establecidos.

Clave consiste en la combinación de letras, números y signas y su largueza no debe ser no más corto de ochos símbolos. No se puede usar como clave los datos identificando la persona (por ejemplo, los Datos personales, número de automóvil, nombres y apellidos de los allegados, nombres que es conexos con el lugar de trabajo o que se usan allí frecuentemente).

Al ingresar la clave por parte del Usuario de las Sistemas de Información, no debe ser visibles para lectura en la pantalla del ordenador.

El Usuario de las Sistemas de información debe cambiar la clave por lo menos una vez en tres meses. El Administrador de las Sistemas de información debe asegurar:

- requerimiento automático del cambio de clave para los Usuarios, la primera vez registrando en la red;
- requerimiento automático del cambio de clave dentro de cados tres meses;
- bloqueo de las sistemas por hasta 1 hora, si el Usuario cinco veces de seguida entra no correcto clave o nombre de usuario.

El Usuario de las Sistemas de información debe memorar la clave. Por escrito las claves permitido almacenar solo en una cerrada caja fuerte.

Si surgen las sospechas que la clave se enteraba la otra persona, el Usuario de las Sistemas de información inmediatamente informa sobre el Incidente al propietario de los Recursos de información, al propietario de los recursos técnicos y al administrador de las Sistemas de información.

Está prohibido intentarlo saber los claves de otros Usuarios, excepto casos, cuando esto es necesito al administrador de las Sistemas de información para realización sus terceras obligaciones. Después de conclusión de mentados trabajos, el usuario de las Sistemas de información cambia la clave.

En la pantalla debe ser establecida la salvapantalla con la clave de autorización. Debe ser activada automáticamente, si durante de cinco minuten el Usuario no realiza ninguna acciones.

11. MEDIDAS QUE SE REALIZAN PARA PROTECCIÓN DE LOS RECURSOS TÉCNICOS CONTRA LOS INCIDENTES EXTRAORDINARIOS Y LOS MEDIOS QUE ASEGURAN LA PROTECCIÓN DE LOS RECURSOS TÉCNICOS CONTRA EL DAÑO INTENCIONADO Y ADMITEN EL RECIBIMIENTO

DLV realiza las medidas de la protección física de las Sistemas de información que defienden sus contra los factores del medio ambiente (incendio, inundaciones, altibajos de la temperatura y otros), de los factores técnicos (la suministra de la electricidad impropia y otros) y los factores humanos (daños intencionados o no intencionados, robo y otros).

Protección física de los servidores:

- DLV asegura que todas Sistemas de información se explotan con el acceso restringido en lugares cerrados, la Protección física de cuales asegura el acceso solo de las personas autorizadas, o asegura la protección física de los servidores, para que no puedan apagarse, cambiar de lugar, causar daño y cambiar su configuración no autorizado. Lugares de los servidores instalan en lugares del edificio en cuales menos probable la realización de las Amenazas;

- Personas no autorizadas, incluyendo los representantes de los servicios externos, en los lugares de servidores pueden estar solo en el acompañamiento de las personas autorizadas;

- En dependencia de la cantidad de pérdidas posible, DLV asegura la protección bastante de los servidores y los locales de servidores contra las Amenazas físicas (incluyendo contra condiciones climatológicas no apropiadas, incendios, inundaciones, interrupción de la suministra de electricidad, daños intencionados), en caso de necesidad instalando la alarma antirrobo y la alarma de incendios, el sistema contra incendios automática, estableciendo los equipos de la alimentación de corriente alternativa y el equipo de condensación del aire.

Para infraestructura de las redes (incluyendo para los aparatos de las redes de comunicación, la red de cables) DLV asegura la protección física bastante, colocando ella tal que no pueden conectarse no autorizado, conectarse libremente a ella o las personas no atadas con DLV dañar, y también no pueden conectarse no autorizado, conectarse libremente a ella y dañar o dañar accidental y de imprudencia por parte de los Empleados o los visitantes de DLV.

Protección física de las estaciones de trabajo:

- Lugar de trabajo del propietario de los Lugares tecnológicos separan los lugares del acceso restringido;

- Las estaciones de trabajo usan de acuerdo a las exigencias establecidas y usan equipos de la suministra de electricidad permanente, si resulta que el riesgo de las violaciones de la suministra de electricidad es inaceptablemente alto.

Protección física de los equipos portátiles:

los ordenadores portátiles usa de acuerdo a las exigencias establecidas por parte del fabricante;

DLV realiza la registración de la circulación de los equipos portátiles, para establecer la que persona usa siguiente equipo.

Protección física de los portadores de datos:

- DLV realiza las necesitas medidas de seguridad para la protección física de todos los portadores de datos con independencia de sus tipos (incluyendo desarmados equipos de discos, impresiones de papel, impresiones en papel de fax, disquetes, discos ópticos y otros);
- Los portadores de datos que tienen los recursos de las Sistemas de información pueden usar o cambiar de lugar sin el límite de tiempo especial solo los Empleados de DLV autorizados que tienen

el acceso a los recursos de las Sistemas de información. Los recursos de las Sistemas de información que no hay la necesidad usar o cambiar de lugar se almacenan en los locales de DLV, en los locales determinados para les. Si es necesidad aniquilar los portadores de datos, el propietario de los Recursos tecnológicos controla y asegura sus aniquilamiento;

- En el contexto de la protección de los portadores de datos, DLV realiza la protección física del equipo de entrada y de salida de datos, eliminando el uso no sancionado – el equipo de impresoras no instalan en locales de acceso público, no admiten la actividad externa de los portadores de datos, si no es necesita para realización de las obligaciones de los Empleados;
- Los portadores de datos con los Recursos de información clasificados están prohibido dejar en los locales inseguros (por ejemplo, del acceso público);
- Si el portador de datos que tiene los Recursos de información clasificados, debe ser destruido, allí esto realizarse en tal modo que no puede ser realizar la renovación en él existentes datos.

En caso de la necesidad DLV realiza las medidas adicionales de la protección física en relación al nivel de clasificación de los recursos del sistema de información. Las medidas de la protección física de las Sistemas de información realizarse sistemáticamente, no admite la situación cuando los recursos de las Sistemas de información estuvieron afuera de los locales de acceso restringido sin control de los Empleados autorizados de DLV. DLV realiza la verificación regular de las medidas de la protección física.

Copias reservas de los datos se fabrican de acuerdo al procedimiento establecido del miembro de la junta de DLV.

En caso de cualquier Incidentes, por ejemplo, robo de los portadores de datos, en caso de desaparición, el Empleado apropiado inmediato informa el propietario de los Recursos Tecnológicos y de Información que realizan todas medidas necesitas para la protección de datos.

12. ORDEN DEL ALMACENAMIENTO Y ANIQUILAMIENTO DE LOS PORTADORES DE INFORMACIÓN

En caso del cierre del sistema de información o antes del aniquilamiento del portador de información, la persona responsable borra un contenido de información, un contenido de las bases de datos, y también todos otros conexos ficheros.

Si es necesario borrar los datos de el sistema de información, DLV asegura la eliminación completa de los datos de el sistema de información completa para que no se puedan recuperar

13. DERECHOS, OBLIGACIONES, LIMITACIONES Y RESPONSABILIDAD DE LOS USUARIOS DE LOS DATOS PERSONALES

Usuarios de las Sistemas de información pueden usar los recursos asignados de los Sistemas de información solo para la realización de las obligaciones de trabajo y pueden procesar los Datos personales solo de acuerdo a los objetivos de su procesamiento y para la realización de las obligaciones de trabajo.

Usuario de las Sistemas de información tiene la responsabilidad por actividades que se realizan, usando su nombre de usuario (identificador). Autenticidad del Usuario de las Sistemas de información se determina para asegurarse que el usuario del nombre de usuario (identificador) es su propietario autorizado. Para determinar la Autenticidad se usan las claves. Después de la entrada del nombre de usuario (identificador) y la clave, el Usuario del sistema de información puede usar los recursos del sistema de información de acuerdo a los derechos de acceso establecidos.

El Usuario de las Sistemas de información debe recordar la clave. La clave por escrito se permitida almacenar solo en una cerrada caja fuerte.

Está prohibido intentar saber las claves de otros Usuarios, con excepción de los casos cuando esto es necesito al administrador de las Sistemas de información para la realización sus obligaciones directas. Después de la conclusión de los trabajos mentados, el Usuario de las Sistemas de información cambia la clave.

A conclusión de las relaciones de trabajo de los Usuarios de las Sistemas de información con DLV, el administrador de las Sistemas de información anula todos derechos de acceso a los recursos de las Sistemas de información.

Usando los recursos de las Sistemas de información, la obligación del Usuario de las Sistemas de información es notificación inmediata del administrador de las Sistemas de información en siguientes casos:

- Si surgen las sospechas que otra persona sabía la clave del Usuario;
- recibiendo unos mensajes de origen desconocido al Correo electrónico (por ejemplo, correspondientes desconocidos, especialmente indicadas temas de mensajes);
- si surgen las sospechas que un ordenador se infecta con el virus, también apagar el ordenador;
- si surgen las sospechas de unos daños de la técnica de ordenador, también inmediatamente apagar la técnica dañada;
- notando las desviaciones de la actividad del ordenador o de el sistema de información;
- si es necesario cambiar la ubicación de la técnica de ordenador;
- leer el aviso, enviados por parte del administrador de el sistema de información, y oportunamente realizar las actividades indicadas;
- familiarizarse con las instrucciones y recomendaciones incorporadas en el catálogo de uso general;
- regularmente borrar los mensajes innecesarias para trabajo del Correo electrónico;
- no interrumpir el proceso de renovación de una programa antiviral;
- mirar para que en el ordenador obligatoriamente es activada la salvapantalla con la protección de la clave. El protector de la pantalla debe ser activado automáticamente, si durante cinco minutes el Usuario no realiza ningún actividades.

El Usuario de las Sistemas de información no está permitido:

- Usar los recursos de las Sistemas de información para difundir o almacenar la información no conexo con el trabajo (por ejemplo, notificación del carácter comercial o personal, exhortaciones, publicidades, programas destructivas, juegos);

- realizar la actividad que carga innecesario los recursos de las Sistemas de información en vista de otros necesidades de los Usuarios de los Sistemas de información (por ejemplo, usar el internet excesivamente, imprimir sin necesidad gran cantidad de copias de documentos, dejar ficheros abiertos disponibles en el servidor de ficheros, cuales no son necesarios para trabajo);

- cargar las programas disponibles en el internet;

- independientemente instalar el software del ordenador;

- transferir no autorizado las copias del software unos datos de trabajo a tercero;

- sin coordinación con el miembro de la junta de DLV crear para sí u otorgar a otros Usuarios el acceso alejado a su estación de trabajo, el ordenador portátil o los recursos del servidor;

- independientemente cambiar la configuración del ordenador, cambiar el lugar de la técnica estacionaria de la oficina y eliminar algunos daños de la técnica de ordenador;

- conectar al sistema del suministro de energía eléctrica constante algunos dispositivos electrónicos, a excepción de los ordenadores, las pantallas y los dispositivos de estampa.

El Usuario de las Sistemas de información tiene la obligación de las pérdidas que surgen por la inobservancia de las exigencias establecidas en estas condiciones.

Administrador de las Sistemas de información:

- crear, modificar y liquidar los identificadores (cuentas) del Usuario de las Sistemas de información y arroga los derechos apropiados;

- si es necesario limita la capacidad del fichero del disco del servidor o algún su catálogo, informando sobre esto todos Usuarios de esto disco o catálogo vía el Correo electrónico;

- controla que los Usuarios de los recursos de las Sistemas de información observan las

condiciones del cambio de la clave establecidas en estas reglas.

Administrador de las Sistemas de información tiene los derechos:

- desconectar los recursos de las Sistemas de información en los fines de semana o afuera las horas de trabajo oficiales, para realizar los trabajos de soporte, 3 días hábiles antes, advertido sobre esto los Usuarios de las Sistemas de información;

- desconectar los recursos de las Sistemas de información y suspender el trabajo de los sistemas también en horas de trabajo, si hubo el accidente (si es posible, avisando por adelanto sobre esto los Usuarios vía teléfono y correo electrónico).

14. PROCEDIMIENTO DE LA VIOLACIÓN DE LA PROTECCIÓN DE LOS DATOS PERSONALES

De acuerdo con los artículos 33 y 34 de la Regula, DLV como el Propietario de los Datos constata, registra, investiga, valora y toma la decisión sobre el aviso de ocurrió la violación de la protección de los Datos personales de Inspección de datos estatal y/o del sujeto de los Datos personales.

1. Reglas generales.

1.1. El Empleado que constató cualquier Violación de la protección de los Datos personales o sus signos, inmediatamente informa sobre esto tanto al propietario de los Recursos de información como de los recursos técnicos.
1.2. En caso de las Violaciones el Empleado dentro de sus posibilidades y autoridades, tiene la obligación asegurar la seguridad de los Recursos técnicos y de la Información entes de momento del aparecimiento del propietario de recursos apropiado.

2. La Registración, la investigación y la valoración de las violaciones

2.1. Recibiendo la información del Empleado que Procesado de Datos, del Compañero de Colaboración o cualquier Tercero sobre la Violación posible, la persona responsable (especialista de la protección de datos) (en adelante – la Persona responsable) inmediatamente verifica, si la información es verdadera. En caso de las sospechas sobre la Violación, ello fijarse inmediatamente en el registro de Violaciones (anexo Nr.1).
2.2. La Persona responsable tiene la responsabilidad de la gestión del registro de Violaciones.
2.3. Después de la registración de las Violaciones, la Persona responsable abre una investigación y determina el tipo de la Violación, las causas de origen y toma la decisión sobre la influencia del riesgo a los derechos del sujeto de datos.
2.4. Existen siguientes tipos de las Violaciones:
  2.4.1. la Violación de la Accesibilidad – (A)
  2.4.2. la Violación de la Integralidad – (B)
  2.4.3. la Violación de la Confidencialidad – (C)
2.5. En caso de varios tipos de la Violación, en registro de Violaciones determina todos apropiadas designaciones de las Violaciones.
2.6. Sobre la Influencia de los derechos y la libertad del sujeto de datos existen siguientes Influencias de la Violación:
  2.6.1. Violación no crea el riesgo o poco probable que el riesgo será creado – (1)
  2.6.2. Violación puede crear el riesgo o creó el riesgo – (2)
  2.6.3. Violación crea alto riesgo– (3)
2.7. Si se constataron varios tipos de las Violaciones con varios Valores de riesgo, la acción en el contexto del aviso sobre la Violación se realiza, tomando a cuenta del más alto Valor de la Influencia del riesgo.
2.8. Después del análisis de la Influencia de la Violación, se toma la decisión sobre el aviso de ello acorde con estas condiciones.
2.9. Adicionalmente con el análisis de la Influencia de la Violación, realiza la eliminación de las consecuencias creadas de la Violación de acuerdo a la Influencia que creí la Violación, en caso de la necesidad interrumpiendo el trabajo de las Sistemas de información.

3. Aviso de Inspección de datos estatal

3.1. Si es poco probable que la Violación puede crear el riesgo de los derechos y la libertad del sujeto de datos (Información sobre el bajo riesgo), el aviso de Inspección de datos estatal no realizarse.
3.2. Si la Violación puede crear el riesgo o alto riesgo de los derechos y la libertad del sujeto de datos, Jefe de Datos comunica sobre la violación de la protección de datos a Inspección de datos estatal inmediatamente, pero a más tardar durante 72 horas de momento, cuando la Violación hizo conocido.
3.3. En el aviso de Inspección de datos estatal, Jefe de Datos indica siguiente:
  3.3.1. describe un carácter de la Violación, incluyendo las categorías y la cantidad aproximada del sujeto de datos;

3.3.2. información de contacto del especialista dela protección de datos u otra información de contacto donde es posible recibir la información adicional;
3.3.3. unas consecuencias probables de la Violación;
3.3.4. Medidas que Jefe de Datos realiza o plana realizar para eliminar la Violación y su consecuencias adversas.

4. Distribución de la información a los sujetos de datos sobre la Violación de la protección de datos

4.1. Si Jefe de datos constata que la Violación puede crear alto riesgo a los derechos y la libertad del sujeto de datos, Jefe de datos inmediatamente sobre esto da a conocer al sujeto de datos.
4.2. En un aviso al sujeto de datos indica la información indicada en el punto 3.3.
4.3. El aviso al sujeto de datos no realizarse, si:
4.3.1. Jefe de Datos realizaba las medidas técnicas y de organización apropiadas de la protección, y las medidas mencionadas se aplica a los Datos personales que afectaba la Violación, especialmente tal medidas que hacen los Datos personales no comprendes a las personas que no tienen poderes del acceso a los datos;
4.3.2. Jefe de Datos después de la Violación hacía actividades técnicas y de organización para no crear alto riesgo al sujeto de datos de sus derechos y libertad;
4.3.3. Si el aviso no exige esfuerzos inadecuados. En esto caso puede ser usaba el aviso público o la comunicación similar que con igual eficiencia informa los sujetos de datos.
4.4. Si surgen las sospechas sobre un delito penal (robo de datos se comete Terceros y otros), Persona responsable después de la consultación con Jefe toma la decisión sobre el aviso a Policía Estatal e Inspección de datos estatal.