#walk15

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

SECCIÓN 1
DISPOSICIONES GENERALES

1. La Política de Tratamiento de Datos Personales (en adelante la Política) de Walk15, UAB (en adelante, la Empresa) es una parte de la Política de Tratamiento de Datos que se hace pública y que regula los propósitos del tratamiento de los datos personales de las personas físicas cuyos datos son procesados por la Empresa, establece los procedimientos para hacer valer sus derechos, fija las medidas organizativas y técnicas de protección de datos y regula la invocación de los procesadores de datos personales.

2. Esta política se elabora en base a lo siguiente:

- Ley de Protección Legal de Datos Personales de la República de Lituania (en adelante LLPPD).
- Reglamento General de Protección de Datos (en adelante GDPR).
- Orden del Gobierno de la República de Lituania del 28 de febrero de 2001 Nº 228 "En relación con la aprobación de la orden de remuneración por el suministro de datos al interesado y la remuneración por la recopilación de datos de los controladores de datos registrados".
- Otra legislación relacionada con el tratamiento y la protección de los datos personales.

3. Esta Política se aplica al tratamiento automático de datos personales de personas físicas, así como al tratamiento manual de conjuntos sistemáticos de datos personales. Esta Política también establece los derechos, obligaciones y responsabilidades de los empleados de la empresa en relación con el tratamiento de datos personales.

4. Los requisitos de esta Política son vinculantes para todos los empleados de la Empresa (en adelante denominados Empleados) y también deben ser cumplidos por los procesadores de datos que, al prestar servicios de procesamiento de datos a la Empresa, tengan conocimiento y procesen datos personales, mientras que no estén regulados por acuerdos separados entre la Empresa y los procesadores de datos.

SECCIÓN 2

CONCEPTOS GENERALES

5. Datos personales / Datos - significa cualquier información relativa a una persona natural identificada o identificable - directa o indirectamente, en particular por referencia a un identificador como un nombre, un código personal, datos de localización, un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona natural.

6. Tratamiento de datos - significa cualquier operación o serie de operaciones realizadas de forma automatizada o no automatizada sobre datos personales o conjuntos de datos personales, tales como la recogida, el registro, la clasificación, la sistematización, el almacenamiento, la adaptación o modificación, la extracción, la familiarización, la utilización, la divulgación mediante la transmisión, la distribución o cualquier otra forma de puesta a disposición para su uso, así como la colación o interconexión con otros datos, la restricción, la supresión o la destrucción.

7. Controlador de datos - Walk15, UAB, quien determina las formas y los medios de uso de los datos al procesar los datos de los interesados.

8. Interesado - Empleados y otras personas físicas cuyos datos son tratados por Walk15, UAB.

9. Procesador de datos - entidades que procesan datos personales controlados por Walk15, UAB, bajo las instrucciones de Walk15, UAB de acuerdo con los contratos de servicio celebrados.

10. Suministro de datos significa la divulgación de datos personales por transferencia u otros medios de puesta a disposición (excluyendo la publicación en los medios de comunicación).

11. Aplicación móvil - La aplicación móvil Walk15 administrada por la Empresa.

12. Administración interna - actividades que garantizan el funcionamiento autónomo del controlador de datos (gestión de la estructura, gestión del personal, gestión y utilización de los recursos materiales y financieros disponibles, mantenimiento de registros).

13. Otros términos utilizados en la Política se entenderán tal y como se definen en la LLPPD y/o el GDPR.

SECCIÓN 3

PRINCIPIOS Y OBJETIVOS DEL TRATAMIENTO DE DATOS PERSONALES

14. En el ejercicio de sus funciones y en el tratamiento de los datos personales, el equipo estará obligado a:

- Tratar los datos personales de forma legal, justa y transparente.
- Recoger los datos para fines específicos, explícitos y legítimos y no tratarlos posteriormente de forma incompatible con dichos fines.

- Observar los principios de celeridad, proporcionalidad y minimización de la cantidad de datos en la recogida y el tratamiento de los datos personales, no exigir el suministro de datos que no sean necesarios, no almacenarlos, y abstenerse de procesar datos en exceso.
- Garantizar la exactitud de los datos personales y, cuando sea necesario para los fines del tratamiento de datos personales, mantenerlos actualizados; corregir, completar, eliminar o suspender el tratamiento de datos inexactos o incompletos.
- Almacenar los datos personales de manera que permitan la identificación de los Interesados durante no más tiempo del necesario para los fines para los que se recogieron y trataron los datos.
- Tratar los datos personales de manera que se garantice una seguridad adecuada de los datos personales mediante la aplicación de medios técnicos u organizativos apropiados, incluida la protección contra el tratamiento no autorizado o el tratamiento ilícito y contra la pérdida, destrucción o daño involuntarios de los datos (principio de integridad y confidencialidad).

15. La Directora de desarrollo regional Justina Verbickaitė es responsable de la actualización de la Empresa de los datos de los Interesados.

16. La información sobre el Interesado debe ser proporcionada si es requerida por la ley.

SECCIÓN 5

TRATAMIENTO DE LOS DATOS DE LOS CANDIDATOS AL EMPLEO

- La Empresa procesa los siguientes datos de las personas que desean participar en el proceso de contratación de la Empresa: nombre, apellido, fecha de nacimiento, dirección, teléfono, correo electrónico, educación, otros detalles especificados en los documentos proporcionados por los candidatos a la Empresa, incluyendo el CV. En el caso de que la legislación de la República de Lituania prevea restricciones adicionales sobre el tipo de información de los candidatos que puede ser procesada, el controlador de datos se asegurará de que sólo se procesen los datos personales permitidos de los candidatos. Los datos sensibles no se procesan a menos que el candidato decida proporcionar estos datos sobre sí mismo.

17. La base del tratamiento de datos es el consentimiento. Los candidatos a las vacantes están dando su consentimiento (por acción concluyente) para el tratamiento de sus datos sólo hasta el final del proceso de selección. Los datos de los candidatos que no hayan sido seleccionados para el puesto (vacante) se eliminarán al final del procedimiento de selección, a menos que den su consentimiento explícito para el tratamiento de los datos al final del procedimiento de selección.

18. La finalidad del tratamiento de datos es la administración interna. Si se obtiene el consentimiento del candidato para el tratamiento de sus datos una vez finalizado el proceso de selección con el objetivo de ofrecerle un futuro puesto de trabajo, los datos se tratarán sobre la base del consentimiento.

19. Los candidatos envían sus datos personales cuando se presentan a la Empresa. En algunos casos, cuando el muestreo se lleva a cabo a través de terceros (procesadores de datos de la Empresa), los datos se proporcionan primero a ellos y sólo después a la Empresa. En todos los casos, la Empresa es el controlador de Datos.

20. Los datos de los candidatos no se divulgarán a terceros a menos que los candidatos lo soliciten y cuando existan motivos legítimos para dicha transferencia.

21. Los datos de los candidatos se procesan sistemáticamente en las bases de datos de la Empresa, cuyo acceso está disponible para los proveedores de servicios informáticos de la Empresa. Los currículos de los candidatos o las cartas de presentación también pueden conservarse en papel.

22. Los candidatos son informados del tratamiento de sus datos y de sus derechos, incluido el derecho a solicitar a la Empresa la supresión de estos. La información se concluirá en la Política disponible públicamente en las páginas web de la Empresa.

SECCIÓN 6

DATOS DE PERSONAS FÍSICAS TRATADOS PARA LA PRESTACIÓN DE SERVICIOS

23. La Empresa puede tratar los siguientes datos de las personas que utilizan el servicio de la Empresa en una App Móvil: nombre, apellidos, sexo, altura, peso, longitud del paso, idioma, correo electrónico, dirección, ubicación, datos que se reciben de los proveedores de servicios de pago (es decir, Google Pay), así como otros datos proporcionados directamente por el Interesado.

24. Los usuarios del servicio aceptan las condiciones de uso de la App Móvil gestionada por la Empresa antes de utilizarla. La base para el tratamiento de datos es la celebración y ejecución del contrato.

25. La finalidad del tratamiento de los datos es prestar los servicios adecuadamente.

26. Los propios Interesados envían sus datos personales o dan a la App Móvil la posibilidad de sincronizar los datos desde Samsung Health, Apple Health Kit u otras aplicaciones móviles. En casos específicos, los datos pueden obtenerse de terceros, por ejemplo, cuando los Interesados realizan compras, los datos proceden de las empresas de servicios de pago o, cuando usted se registra con su cuenta de Google o Facebook, los datos proceden directamente de estas empresas.

27. Los datos se almacenan en las bases de datos de la empresa, a las que tienen acceso las empresas que prestan servicios informáticos a la empresa. Los datos no se divulgarán a otros terceros a menos que se obtenga una solicitud para ello y cuando existan motivos legítimos para dicha transferencia.

Cuando los Interesados utilicen determinadas funciones de la aplicación Móvil (por ejemplo, la participación en un reto), sus datos podrán estar disponibles públicamente en la aplicación Móvil, pero en todos los casos, podrán desactivar esta función y participar de forma anónima.

Los datos también pueden proporcionarse a terceros que, en colaboración con la Empresa, publican sus ofertas en la aplicación Móvil ("Step Wallet"). Los datos se facilitan cuando un usuario de la aplicación móvil decide utilizar la función Step Wallet.

28. Los Interesados son informados del tratamiento de sus datos y de sus derechos. La notificación se hará en la Política disponible públicamente el sitio web de la empresa y en la aplicación móvil, así como las normas de uso, previstas en la aplicación móvil.

SECCIÓN 7

TRATAMIENTO DE DATOS CON FINES DE MARKETING DIRECTO

29. A efectos de marketing directo, la empresa trata los siguientes datos personales: nombre, apellidos, dirección de correo electrónico. También pueden tratarse otros datos de contacto.

30. El tratamiento de datos se basa en el consentimiento.

31. Los propios Interesados presentan sus datos personales a la empresa.

32. Los datos se almacenan en las bases de datos de la Empresa, a las que tienen acceso las empresas que prestan servicios informáticos a la Empresa. Los datos no se divulgarán a otros terceros a menos que se obtenga una solicitud para ello del Interesado y cuando existan motivos legítimos para dicha transferencia.

33. La Empresa no trata datos de menores ni datos personales sensibles para este fin. No obstante, cuando se recopilan datos con fines de marketing directo, la Empresa no verifica la edad de los interesados, ya que se trataría de un exceso de recopilación de datos.

34. Los Interesados son informados del tratamiento de sus datos y de sus derechos, incluido el derecho a solicitar a la Empresa la supresión de los datos. La notificación se hará en la Política, se divulgará públicamente en la página web de la Empresa y en la Aplicación Móvil. Los Interesados, una vez descargada y utilizada la App Móvil, tienen derecho a aceptar que se les envíen boletines de marketing directo por correo electrónico o por otras vías facilitadas por el Interesado. El Interesado tiene derecho a anular la suscripción o a cancelar esta opción en cualquier momento.

SECCIÓN 8

TRATAMIENTO DE DATOS PARA CONSULTA, SOLICITUD O GESTIÓN, EVALUACIÓN Y EXAMEN DE RECLAMOS

35. La Empresa podrá procesar los siguientes datos de las personas físicas que se pongan en contacto con ella para la finalidad especificada: nombre, idioma, correo electrónico. dirección. La Empresa también puede procesar otros datos obtenidos directamente del Interesado y necesarios para la investigación, administración o evaluación de la solicitud, consulta o queja.

36. La base para el tratamiento de datos es la celebración y ejecución del contrato.

37. Los propios interesados presentan sus datos personales.

38. Los datos se almacenan en las bases de datos de la Empresa, a las que tienen acceso las empresas que prestan servicios informáticos a la Empresa. Los datos no se divulgarán a otros terceros a menos que se obtenga una solicitud para ello de los Interesados y cuando existan motivos legítimos para dicha transferencia.

39. Los Interesados son informados del tratamiento de sus datos y de sus derechos. La notificación se hará en la Política, se divulgará públicamente en la página web de la empresa y en la Aplicación Móvil.

SECCIÓN 9

COOKIES

40. La Empresa utiliza cookies para mejorar la navegación y los servicios prestados por el sitio web Walk15.com. El sitio web de la Compañía puede utilizar cookies analíticas de terceros: "Google Analytics".

41. En el sitio web de la Empresa se utilizan o pueden utilizarse las siguientes cookies.

Nombre del cookie	Descripción	Momento de creación	Caducidad	Datos usados
_ga	Se registra una ID única que se usa para generar estadísticas sobre el uso del sitio por los visitantes.	Al hacer clic en el botón "Acepto"	2 años	Identificador único
_gid	Esta cookie se utiliza para distinguir a los usuarios.	Al hacer clic en el botón "Acepto"	24 horas	Identificador único
_gat*	Estas cookies se utilizan para limitar el número de solicitudes.	Al entrar en la página	10 min	Identificador único
cookieconsent_status	Se utiliza para guardar el consentimiento del usuario para usar cookies.	Al hacer clic en el botón "Acepto"	1 año	Identificador único
pll_language	Esta cookie se utiliza para guardar el idioma preferido por el visitante.	Al entrar en la página	1 año	Idioma

42. La empresa puede recoger datos sobre las acciones de los visitantes y sus hábitos de navegación en un sitio web.

43. Para más información, puede ver: http://www.google.com/analytics.

44. Para saber cómo desactivar el seguimiento de las páginas web con cookies de Google Analytics, visite: http://tools.google.com/dlpage/gaoptout.

45. Los datos se transmiten a los proveedores de servicios informáticos y a Google. Los datos no se divulgarán a otros terceros a menos que se obtenga una solicitud para hacerlo y cuando haya motivos legítimos para dicha transferencia.

46. El sitio web le permite rechazar el uso de cookies.

SECCIÓN 10

TÉRMINOS DE ALMACENAMIENTO DE DATOS

47. El responsable del tratamiento aplicará los siguientes plazos de conservación de los datos personales:

No.	Purpose of processing of personal data	Term of storage
1.	Processing of employee data for the purposes of internal administration.	Up to 50 years after the end of the employment contract, in accordance with the Index for retention periods in the General documentation.
2.	Processing of personal data of job candidates.	Until the end of selection.
3.	Processing of personal data of job candidates after the end of the selection takes place after obtaining permission to process data.	Two years from the date of receipt of the curriculum vitae.
4.	Provision of services.	Data shall be processed for a period which shall not exceed 10 years, as laid down by law.
5.	Administration, evaluation and examination of requests, inquiries or complaints.	6 months from the date of receipt of the request.
6.	For direct marketing purposes.	3 years from obtaining consent.
7.	Cookies to improve the quality of your use of the site.	The length of time a cookie stays on your computer depends on the type of cookie.

48. Exceptions to the above retention periods may be determined insofar as such exceptions do not violate the rights of the Data subjects, meet legal requirements and are properly documented.

SECCIÓN 11

DATA SUBJECTS RIGHTS AND PROCEDURES FOR THEIR IMPLEMENTATION

Ensuring Data subjects' rights and awareness

49. Data subjects have the right to:

- To know (be informed) about the processing of their personal data.
- By submitting to the Company an identity document or by electronic means that allows the person to be properly identified – to access their personal data and its processing, to obtain information on the sources and what specific personal data is collected, the purpose for which it is processed, the recipients at least in the last 1 year, in addition – to receive a copy of the documents containing their personal data.

- Require the rectification, erasure or restriction of personal data except for storage where the processing is in breach of legal requirements.

- To object to the processing of their personal data.

- To request transfer of data to another data controller or to provide it directly to the Data subject in a form that is convenient for the Data subject (such data provided to the Company by the Data subject itself).

- Lodge a complaint with the supervisory authority.

- Revoke consent (if personal data is processed on the basis of consent).

50. In all cases, the Company must provide the Data subject with information (unless the Data subject already has such information) about:

- Its name, legal entity code and registered office.

- Contact details of the data protection officer, if any.

- For what purposes and on what legal basis is the personal data of the Data subject processed.

- The recipients of the data and their categories.

- The period for which the data will be stored or the criteria used to determine that period.

- Other additional information (what of the Personal Data must be provided by the Data subject and the consequences of failure to provide the data, about the Data subject's right of access to his or her personal data and his right to correct incorrect, incomplete, inaccurate personal data) in the volume that is needed, in order to ensure the proper personal data processing without the violation of the rights of the Data subject.

- The communication of his personal data to third parties at the latest at the time the data are first provided during the first time and if the Data subject was unaware that the data will be transferred to another party.

Order for the implementation of data subjects' rights

51. The Company is obliged to:

- Enable the Data subject to exercise the specified rights of the Data Subject, except as in cases stipulated by law, when it is necessary to ensure national security or defense, public order, crime prevention, investigation, detection or criminal prosecution, important state economic or financial interests, prevention of violations of service or professional ethics, its investigation and detection, protection of the rights and freedoms of the Data subject or other persons.

- Data subjects must contact the Company branch to exercise their rights at the following contacts: info@walk15.lt.

- The Company must ensure that all necessary information is provided to the Data subject in a clear and comprehensible manner.

- The Data subject must reply no later than in 20 (twenty) business days from the date of receipt of the request. If the Data subject is refused access to the data, he shall be given a reasoned and substantiated reply regarding the non-execution of his request.

52. The Company shall immediately inform the data recipients of the personal data, which was corrected or destroyed at the request of the data subject, the suspended processing of personal data, unless the provision of such information would be impossible or excessively difficult (due to the high number of data subjects, data period, unreasonably high costs). In this case, the State Data Protection Inspectorate must be notified immediately.

53. The Company shall provide the data to the Data subject free of charge. In certain cases (whenever the Data subject clearly abuses his rights, submits unreasonably repeated requests for information, excerpts, documents), such provision of information and data to the Data subject may require remuneration in accordance with legal requirements and the rates set by the Company.

Provision of data-to-data recipients

54. The Company shall provide the Data of the Data subject according to the requirements of the legal acts and while ensuring their confidentiality.

55. In the case of one-time data provision, the Company shall give priority to the provision of information by electronic means.

56. The provision of personal data to state and municipal institutions and bodies, when such institutions and bodies receive personal data for the performance of the statutory control functions, shall not be considered as the provision of data to recipients.

SECCIÓN 12

ORGANIZATIONAL AND TECHNICAL MEASURES FOR PERSONAL DATA PROTECTION

57. The Company makes every effort to ensure that the Company's organizational and technical data security measures comply with GDPR requirements. The following infrastructural, administrative and telecommunications (electronic) measures shall be taken to protect personal data against accidental or unlawful destruction, alteration, disclosure or any other unlawful processing:

- Proper hardware layout and maintenance, information systems maintenance, network management, ensuring Internet usage security and other information technology measures:

- Access to Data and the right to carry out Data processing operations shall be granted only to the Employees who need access to the personal data in the context of their duties and performed work functions.

- Ensuring security of premises where personal data is stored (only authorized persons have access to concerned premises).

- After assigning a computer or electronic communication device to a particular Employee, such computer / electronic communication device (s) must be password protected. Passwords must be changed periodically, as well as in the presence of certain circumstances (changes of employee, threat of hacking, suspicion that the password has become known to third parties, etc.).

- Ensuring the protection of personal data against unauthorized access to the internal computer network by electronic means of communications.

- Ensuring the use of secure protocols for the transmission of personal data through external data communication networks.

- Strict adherence to safety standards issued by the security service;

- Proper organization of work and other administrative measures;

- The necessary data security measures are installed taking into account the results of the risk assessment;

- Backup and recovery of data;

- Ensuring that data is restored from the latest available backup copies in the event of loss of data Due to hardware failure, software error or other data integrity violation;

- other means.

58. The Company's Regional Development Manager Justina Verbickaitė is responsible for the implementation, control and enforcement of these organizational and technical data security measures.

59. Employees who process personal data must observe the principle of confidentiality and keep any relevant information they have accessed in the course of their duties confidential. This obligation shall continue to apply after transfer to another position within the Company or upon termination of the employment or contractual relationship with the Company.

60. Employees may process personal data in an automatic way only after they have been granted access to the relevant information system. Access to personal data may only be granted to a person who needs personal data to perform his functions. Upon termination of employment relationships, the Employee's rights to access registers and other programs shall be revoked.

61. Employees may transfer documents containing personal data only to Employees who are entitled to work with personal data under duties or separate assignments.

62. Employees performing Data subject's Data processing functions, shall prevent accidental or unauthorized processing, and shall maintain records in a proper and secure manner (avoiding unnecessary storage of the Data Subject's data, etc.). Copies of documents containing data of the Data subject shall be destroyed in such a way that the contents of such documents cannot be reproduced and their contents identified.

63. Employees whose computers store the Data or whose computers are enabled to access the Company's information systems where the Data is stored must use passwords on their computers; "Guest" type user accounts in such systems, i. e. no-password accounts are prohibited. These computers also need to use a screen saver with a password.

64. Unless necessary, files with Data need not be digitally duplicated, i.e., copies of them being made to local computer disks, removable media, remote file storage, etc.

65. The security control and erasure of personal data contained in external data storage media and electronic mail after their use is ensured by transferring them to databases.

66. Regional development manager Justina Verbickaitė must ensure:

- control of unauthorized access to server premises;
- protection of the Company's internal computer network.

67. Employees must organize their work in such a way as to limit the access of other persons to the personal data processed as much as possible. This provision shall be implemented:

- By refraining from leaving documents with processed personal data or a computer that can open files containing personal data, without supervision, so that information contained therein can be read by Employees who are not authorized to work with specific personal data, students or other persons;
- By storing documents in such a way that they (or their fragments) cannot be read by accidental persons;
- If documents containing personal data are transmitted to other Employees, units, branches, offices via persons who are not authorized to process personal data, or by post or courier, they must be transmitted in a sealed opaque envelope. This paragraph shall not apply where such messages are issued personally and confidentially.

68. Regional Development Manager Justina Verbickaitė is responsible for managing and responding to personal data breaches.

SECCIÓN 13

FINAL PROVISIONS

69. The Company has the right to change Privacy Policy at any time. The changes made are valid from the time the Privacy Policy is updated on the website https://walk15.lt/en/privacy-policy/. The Data Subjects are always recommended to read the updated Privacy Policy.