

PRIVACY NOTICE

- ONLINE ACTIVITIES -

1. INTRODUCTION

As a data controller your privacy is important to Splendex (hereinafter: „*Controller*”). This statement (hereinafter: „*Privacy Notice*”) tells you in a transparent way what to expect us to do with your personal information when you use one of our online services or visit our websites. Please read the below details carefully and contact us before exercising your rights. This Privacy Notice does not apply to information collected through others means such as in person. Our website may contain links to third-party websites. We are not responsible for the security, privacy practices, the content, etc. of such websites. If you visit a website from a link on Splendex’s website this Privacy Notice does not apply. The privacy terms of the visited website will govern the use of that website.

Relevant applicable laws:

- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR);
- Act CXII of 2011 on information self-determination and freedom of information (Infotv.).

2. CONTROLLER

Company: Splendex Kft.

Seat: H-7635 Pécs, Lepke dűlő 4. A. ép. TT 3.

Address1: H-1055 Budapest, Szent István körút 15.

Address2: H-7621 Pécs, Irgalmasok utcája 5.

Reg. no.: Cg. 02-09-082432

Represented by: Levente Székely managing director

Phone: +36 30 409 8960

Email: hello@splendex.io

Website: www.splendex.io

3. PRINCIPLES

Personal data may be processed only for specified and explicit purposes, exercising of certain rights and fulfilment of obligations. The purpose of processing must be satisfied in all stages of data processing operations; recording of personal data shall be done under the principle of lawfulness and fairness („*lawfulness, fair procedure and transparency*”).

The personal data processed must be essential for the purpose for which it was recorded, and it must be suitable to achieve that purpose. Personal data may be processed to the extent and for the duration necessary to achieve its purpose („*purpose limitation*”).

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed („*data minimisation*”).

The accuracy and completeness, and - if deemed necessary in the light of the aim of processing - the up-to-dateness of the data must be provided for throughout the processing operation, and shall be kept in a way to permit identification of the data subject for no longer than is necessary for the purposes for which the data were recorded („*accuracy*”).

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data shall preserve its personal character until connection thereof with the data subject may be restored. Connection may be restored with the data subject if the controller has the technical conditions necessary for the restoration. („*storage limitation*”).

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures („*integrity and confidentiality*”).

The Controller shall be responsible for, and be able to demonstrate compliance with the above principles („*accountability*”).

4. DEFINITIONS

„*data subject*” means natural person identified or identifiable by any information;

„*personal data*” means any information relating to the data subject;

„*consent of the data subject*” means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

„*controller*” means the natural or legal person, and the organization without legal personality which - within the framework determined by Act or legally binding act of the European Union - alone or jointly with others, determines the purposes and means of the processing of personal data, makes and executes decisions concerning data processing (including the means used) or have it executed by a data processor;

„*data processing*” means any operation or the totality of operations performed on the data, irrespective of the procedure applied; in particular, collecting, recording, registering, classifying, storing, modifying,

using, querying, transferring, disclosing, synchronising or connecting, blocking, deleting and destructing the data, as well as preventing their further use, taking photos, making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples, iris scans;

„*data transfer*” means ensuring access to the data for a third party;

„*data process*” means overall data processing operation performed by the data processor on behalf of or by the will of the controller;

„*processor*” means the natural or legal person, or organization without legal personality which - within the framework and with the conditions determined by Act or legally binding act of the European Union - performs data processing operation on behalf of or by the will of the controller;

„*third party*” means the natural or legal person, or organisation without legal personality other the data subject, controller, processor and persons who, under the direct authority of the controller or processor process personal data;

„*personal data breach*” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, publication of, or access to, personal data transmitted, stored or otherwise processed;

„*profiling*” means any form of automated processing of personal data consisting of the use of personal data to evaluate, analyse or predict personal aspects relating to a natural person, in particular aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

„*recipient*” means a natural or legal person, or organisation without legal personality to which the personal data are made accessible by the controller or the processor.

„*EEA State*”: means any Member State of the European Union and any State Party to the Agreement on the European Economic Area, as well as any state the nationals of which enjoy the same legal status as nationals of State Parties to the Agreement on the European Economic Area on the basis of an international agreement concluded between the European Union and its member states and the state which is not party to the Agreement on the European Economic Area;

„*third country*”: means any state that is not an EEA State.

5. HOW DO WE MANAGE YOUR PERSONAL DATA?

5.1. NEWSLETTERS	
The purpose of data processing:	<p>sending regular electronic messages containing advertisements and providing information about current promotions, new services, professional articles</p>

The legal basis for data processing:	consent of the data subject (Art. 6 (1) (a) GDPR)
<i>The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</i>	
The categories of personal data concerned:	name (optional), email
The duration of data processing:	until the consent is withdrawn, i.e. until you cancel subscription
The source of personal data:	subscriber
Consequences of failure to provide data:	it is not possible to subscribe to the newsletter
The method of data processing:	electronic
The existence of automated decision-making, including profiling:	based on your consent, we will perform profiling in order to provide you with offers tailored to your needs, wishes and interests

5.2. ELECTRONIC COMMUNICATION	
The purpose of data processing:	we would like to give a substantive response to your electronic request
The legal basis for data processing:	consent of the data subject (Art. 6 (1) (a) GDPR)
<i>The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</i>	
The categories of personal data concerned:	name, email, phone (optional), content of the message
The duration of data processing:	until the withdrawal of the consent or until 5 years after receipt of the message

The source of personal data:	user initiating the connection
Consequences of failure to provide data:	it is not possible to contact us via the online application form
The method of data processing:	electronic
The existence of automated decision-making, including profiling:	-

5.3. SCHEDULING A BUSINESS MEETING	
The purpose of data processing:	we provide our future clients opportunity to book an appointment for a business meeting via the website
The legal basis for data processing:	consent of the data subject <i>(Art. 6 (1) (a) GDPR)</i>
<i>The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</i>	
The categories of personal data concerned:	name, email, subject of the meeting
The duration of data processing:	until the withdrawal of the consent or until the date of the meeting
The source of personal data:	future client initiating the meeting
Consequences of failure to provide data:	it is not possible to book an appointment for a business meeting via the website
The method of data processing:	electronic
The existence of automated decision-making, including profiling:	-

5.4. RECRUITING	
The purpose of data processing:	selecting a new employee, creating an employment contract, keeping in touch
The legal basis for data processing:	consent of the data subject <i>(Art. 6 (1) (a) GDPR)</i>
	processing is necessary to take steps at the request of the data subject prior to entering into an employment contract <i>(Art. 6 (1) (b) GDPR)</i>
<i>The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</i>	
The categories of personal data concerned:	data voluntarily provided in the tender
The duration of data processing:	until the withdrawal of the consent or, with the specific consent of the applicant, for 1 year from the submission
The source of personal data:	applicant
Consequences of failure to provide data:	you cannot apply for the advertised position
The method of data processing:	electronic
The existence of automated decision-making, including profiling:	evaluation of professional knowledge, competences, assessment of suitability in order to establish an employment relationship, if necessary by implementing profiling

5.5. SOCIAL MEDIA FAN PAGES	
The purpose of data processing:	followers may have the opportunity to learn about the latest professional and marketing content of our company

The legal basis for data processing:	consent of the data subject (Art. 6 (1) (a) GDPR)
<i>The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</i>	
The categories of personal data concerned:	depending on profile settings, follower's public name, profile picture, comment, any data, information, image, video, etc. shared or published via social media
The duration of data processing:	until the withdrawal of the consent or no later than the termination of the fan page or the deletion of the user profile
The source of personal data:	follower (social media user)
Consequences of failure to provide data:	you will not be immediately notified of content shared on fan pages
The method of data processing:	electronic

Social networks generally have the ability to comprehensively analyze your user behavior when you visit their websites or sites with integrated social media content (e.g. like buttons or banner advertisements). Visiting our social media presences will trigger a number of processes which are relevant to data privacy. In detail:

When you log in to your social media account and visit us on this social media platform, the operator of this social media portal has the ability to associate this visit with your user account. However, your personal data can also under certain circumstances be detected even if you are not logged in or do not possess an account with the social media portal in question. In such cases these data can be acquired for example via cookies which are stored on your terminal device, or by acquiring your IP address.

With the aid of data acquired in this way, the social media portal operator can create user profiles in which your preferences and interests are stored. In this way, advertising tailored to your interests can be displayed to you both within and outside of the respective social media presence. If you have an account with the social network in question, advertisements tailored to your interests can be displayed on all devices to which you are or have been logged in.

Please note that despite sharing joint responsibility with the social media portal operator, we have no comprehensive influence over the data processing activities conducted by social media portals. The opportunities open to us are essentially dependent on the corporate policy of the respective provider. Please also note that we are unable to replicate all data processing activities on social media portals. Dependent on the provider, it may be that other processes are performed by social media portal operators. For details, please refer to the data privacy policies of the respective social media portals.

- [Facebook](#)
- [Instagram](#)

- [Linkedin](#)
- [Twitter](#)

5.6. COOKIES

This website uses cookies. We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Cookies are small text files that can be used by websites to make a user's experience more efficient. Cookies are typically categorized as "session" cookies or "persistent" cookies. Session cookies help you navigate through the website efficiently, keeping track of your progression from page to page so that you are not asked for information you have already provided during the current visit, or information needed to be able to complete a transaction. Session cookies are stored in temporary memory and erased when the web browser is closed. Persistent cookies on the other hand, store user preferences for current and successive visits. They are written on your device's hard disk, and are still valid when you restart your browser. We use persistent cookies, for example, to record your choice of language and country location. This site uses different types of cookies. Some cookies are placed by third party services that appear on our pages.

Performance Cookies are used for the following purposes:

- to help us route traffic between servers;
- to understand how quickly features load for users;
- to identify and resolve user experience issues and improve website operations;
- to resolve member inquiries and help ensure compliance with our member rules; and
- to count the number of users of our site.

Preference Cookies are used for the following purposes:

- to enable the website to provide enhanced functionality and personality;
- to allow Sites to remember information that changes the way the site behaves or looks;
- to carry information across pages and avoid having to re-enter information; and
- to allow you to access stored information within session.

Analytics Cookies are used for the following purposes:

- to compile aggregated statistics that allow us to improve the structure of our website;
- to help us better understand how people interact with properties of the website and applications; and
- to help us to determine what product ads are most relevant.

Security and Authentication Cookies are used for the following purposes:

- to authenticate users and prevent fraudulent use of credentials;
- to protect user data from unauthorized parties;
- to provide security within shopping baskets or transactions; and
- to prevent activity that violates our policies.

Targeting and Advertising Cookies are used for the following purposes:

- to allow us to tailor content or advertisements to match your preferred interests or to avoid showing the same advertisements repeatedly;
- to help measure the performance of marketing campaigns; and
- to get insight into how people use our products.

The law states that we can store cookies on your device according to our legitimate interest (Art. 6 (1) (f) GDPR) if they are strictly necessary for the operation of this site. For all other types of cookies we need your permission (Art. 6 (1) (a) GDPR). You can at any time change or withdraw your consent from the pop-up cookie banner on our website. If you do not want Splendex to place cookies on your device, you can also refuse the use of cookies through your browser's settings. You need to separately adjust the settings for each browser and each computer. The links below will take you directly to your browser's user guide. Please note that, if you adjust the cookie settings, you may not be able to correctly use some parts of this website afterwards.

- [Chrome](#)
- [Firefox](#)
- [Internet Explorer](#)
- [Safari](#)

Web Beacons and Pixels

Splendex also collects non-personally identifiable information through the use of tracking pixels that appear on our pages. A tracking pixel is a transparent graphic image (usually 1 x 1 pixel or Javascript tag) that is placed on a web page and, in combination with a cookie, allows us to collect information regarding the use of the web page that contains the tracking pixel. We use tracking pixels to trigger ads on participating websites based on activity tracked from the browser on a device used to visit Splendex website. We also use them to tell when an advertisement we run on another website has been clicked on by Splendex website visitors and use that information to judge which advertisements are more appealing to users. Pixels can also be used for third party web analytics. To opt out of these tracking pixels and services, please follow this link to opt out of:

- the Google Analytics-based tools (<https://tools.google.com/dlpage/gaoptout/>),
- the Facebook Pixel (<https://www.facebook.com/settings?tab=ads>),
- and the Bing Pixel (<https://choice.microsoft.com/en-US/opt-out>).

6. RECIPIENTS

Our staff needs basic access to your personal data as far as it is necessary for the described purposes and the work of the employees concerned. They act in accordance with our instructions and are bound to confidentiality and secrecy when manage your personal data. Additionally, we may disclose your personal data to other recipients if this is so required by national law. Therefore, we also reserve the right to share your personal data in accordance with a court order, official decision or to assert or defend legal claims or if we consider it necessary for other legal reasons.

We may also disclose your personal data to third party processors. Processors are obliged to process the personal data exclusively on our behalf and according to our instructions. Such recipients of your personal data may be located abroad including in countries outside of the EEA. If we disclose your personal data to recipient located in such a third country, we will take appropriate measures to ensure the protection of your personal data, for example by concluding a data transfer agreement. If we transfer personal data to recipients located in so-called third countries, we will ensure - before the start of processing - that the recipient has an adequate level of data protection through appropriate (contractual) guarantees or recognized agreements, or that you as the data subject have given informed consent to the processing of personal data in the respective third country. The Controller intends to transfer personal data to a third country in some cases. The recipients of personal data in third countries are primarily providers of mailing services, data and file storage, analytical tools (see our cookie disclaimer), discussions and direct marketing services.

DATA PROCESSOR	WEBSITE	SERVICE
Calendly	https://calendly.com/	calendar management
MailChimp	https://mailchimp.com/	newsletters
DigitalOcean	https://www.digitalocean.com/	web hosting
SpinupWP	https://spinupwp.com/	web hosting
Mailgun	https://www.mailgun.com/	email
G Suite	https://workspace.google.com/	email
Amazon Web Service (AWS)	https://aws.amazon.com/	backups
Capsule	https://capsulecrm.com/	CRM system

Katalin Szabó E.V.	http://hr-szolgalatasok.hu/	recruiting
--------------------	---	------------

7. SECURITY

Splendex protects the data in proportion with the risks in particular against unauthorized access, alteration, transfer, publishment, deletion or destruction, accidental destruction and loss and against inaccessibility from the change of applied technique. We apply strict security measures to protect the confidentiality, integrity, and availability of your personal data when transferring, storing, or processing it. We use physical, administrative, and technical security measures to reduce the risk of loss, misuse, or unauthorized access, disclosure, or modification of your personal data. All personal data is stored on secure servers operated by Splendex or our partners with access limited to authorized staff only. Splendex protects the electronically processed data with firewalls, antivirus programs, encryption mechanisms, content filter and other technical and process solutions, executes backups in order to prevent data loss and corruption and ensures that, in case of malfunctioning, the systems installed can be restored. The Controller continuously monitors and registers the personal data breaches.

8. RIGHTS OF DATA SUBJECTS AND EXERCISE THEREOF

Your rights enlisted below shall be exercised by submission of your application to the Controller. Section 2 of this Privacy Notice contains the contact information of the Controller. The Controller shall provide information on action taken on a request to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, considering the complexity and number of the requests. Where the Controller has reasonable doubts concerning the identity of the natural person making the request, the Controller may request the provision of additional information necessary to confirm the identity of the data subject. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Controller may either charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or refuse to act on the request. Please note that depending on the nature of the data processing activity, the exercise of certain rights may be impeded.

8.1. ACCESS TO THE PERSONAL DATA

The data subject may request the Controller to provide him or her access to the personal data concerning him or her, including a copy of the personal data which are the subject of the data processing. The data subject has the right to obtain from the Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, has the right to access the personal data and the following information:

- a) the purposes of the processing;
- b) the categories of personal data concerned;
- c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- e) the existence of the right to request from the Controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- f) the right to lodge a complaint with a supervisory authority;
- g) where the personal data are not collected from the data subject, any available information as to their source;
- h) the existence of automated decision-making, including profiling, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

8.2. RIGHT TO RECTIFICATION

The data subject shall have the right to obtain from the Controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

8.3. RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN)

The personal data shall be erased if:

- a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
- c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing;

- d) the personal data have been unlawfully processed;
- e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Controller is subject;
- f) the personal data have been collected in relation to the offer of information society services.

8.4. RIGHT TO RESTRICTION OF PROCESSING

Upon request of the data subject, the Controller will restrict data processing where one of the following applies:

- a) the accuracy of the personal data is contested by the data subject, for a period enabling the Controller to verify the accuracy of the personal data;
- b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- c) the Controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- d) the data subject has objected to processing pending the verification whether the legitimate grounds of the Controller override those of the data subject.

A data subject who has obtained restriction of processing shall be informed by the Controller before the restriction of processing is lifted. The Controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Controller shall inform the data subject about those recipients if the data subject requests it.

8.5. RIGHT TO DATA PORTABILITY

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- a) the processing is based on consent or on a contract; and
- b) the processing is carried out by automated means.

In exercising his or her right to data portability as stated above, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. The exercise of this right shall be without prejudice to the right to erasure.

8.6. RIGHT TO OBJECT

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her unless the processing is carried out for a legitimate interest pursued by the Controller or by a third party or the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, including profiling based on those provisions. The Controller shall no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or if the processing is conducted for the establishment, exercise or defence of legal claims.

8.7. DATA SUBJECT'S RIGHTS DURING AUTOMATED DECISION-MAKING

The data subject shall have the right not to be subject to a decision based solely on automated processing – including profiling – which produces legal effects concerning him or her, or similarly significantly affects him or her. This provision shall not apply if the decision:

- a) is necessary for entering into, or performing a contract between the data subject and the data controller;
- b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms, and legitimate interests; or
- c) is based on the data subject's explicit consent.

In this case, the Controller shall implement suitable measures to safeguard the data subject's rights and freedoms, and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view, and to contest the decision.

8.8. PROCEDURE OF THE NATIONAL AUTHORITY

It is possible for anyone (not only for the data subject) to initiate an investigation or a data protection authority procedure with the Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) on the grounds that a breach of law has occurred or is imminent in connection with the processing of personal data. It is important that the notification shall not be anonymous; otherwise the authority may reject the

notification without a substantive examination. The investigation by the authority is free of charge, and the costs of the investigation are advanced and borne by the authority.

Authority: Nemzeti Adatvédelmi és Információszabadság Hatóság

Seat: 1055 Budapest, Falk Miksa utca 9-11.

Address: 1363 Budapest, Pf. 9.

Phone: +36 1 391 1400

Fax: +36 1 391 1410

Email: ugyfelszolgalat@naih.hu

Website: <http://www.naih.hu>

8.9. RIGHT TO AN EFFECTIVE JUDICIAL REMEDY

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, each data subject has the right to an effective judicial remedy where he or she considers that his or her rights under GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with GDPR. The Controller and the processor shall be obliged to prove that the processing is in accordance with the provisions on data protection determined in legislation or legally binding act of the European Union. In Hungary regional courts have jurisdiction over these actions. The action may also be brought before the court of the domicile or place of residence of the data subject (www.birosag.hu/torvenyszekek). Any person who otherwise do not have legal capacity may be a party in the lawsuit. The authority may join to the data subject in the lawsuit.

9. FINAL PROVISIONS

Please keep in mind, that we are not responsible for the authenticity or accuracy of the data you provide us. The Controller may update this Privacy Notice from time to time as it undertakes new personal data practices or adopt new privacy policies. Amendments of the Privacy Notice shall enter into force simultaneously with the publishing on this website.

Last update: 1 March 2021
