Statement on the use of the recruitment platform 'PitchYou' in line with data protection requirements

The protection of personal data is particularly important in the context of application procedures. Applicants are increasingly given the option of contacting companies online. And it is exactly in this scenario that data protection plays a major role. With PitchYou, potential employees can even apply via WhatsApp.

Whenever external service providers or services are used, data protection compliance must be reviewed. If application data is misused due to a lack of data protection, applicants would be vulnerable and possibly exposed to high risks such as identity theft.

In the following, we would like to inform you that you as a company can integrate the recruitment application PitchYou into your application process in a GDPR-compliant way.

1 General information on data protection

Personal data may only be processed in a comprehensible, i.e. transparent, manner. This is based on Article 5 (1) (a) of the GDPR. Therefore, applicants must be informed about the (planned) processing of their personal data pursuant to Article 13 of the GDPR. Both PitchYou and you as a company comply with this obligation by making applicants aware of the privacy policies when explaining the first steps of the application process via PitchYou. However, it is assumed here that you have expanded your privacy policy to include applicant data and the use of PitchYou. PitchYou will provide you with verified suggested wording for this.

When using WhatsApp, the phone book and contact book are synchronised. Data is then automatically transferred to the USA. In terms of data protection, this is problematic, as generally, very few contacts agree to transmission to WhatsApp or to third countries. Users who personally use WhatsApp have already consented to this in the T&Cs. However, those who don't use it have not.

With the WhatsApp Business API, PitchYou relies on a privacy-friendly solution, as a smartphone is not required on your side in the company in order to communicate with applicants. This excludes address book matching. 'External' data is therefore not transmitted to WhatsApp.

Furthermore, data processing must be lawful. Legitimation facts are outlined in Article 6 of the GDPR. Before applicants can contact you via WhatsApp, opt-in consent is obtained. This is done on the start page, which loads when the QR code is scanned or the link is opened. This therefore excludes applications without consent.

As the processing of personal data is based on consent, the applicant has the right to withdraw their consent at any time pursuant to Article 7 (3) of the GDPR. With PitchYou, the applicant always retains full control over communication and their data. If the applicant decides not to communicate via WhatsApp, they can cancel the communication at any time and use an alternative means of communication (e.g. online form or e-mail).

0391 55 68 63 20 info@lgd-data.de www.lgd-data.de Rogätzer Straße 8 | 39106 Magdeburg

If the applicant wishes to withdraw their application altogether, they have the option of ending the communication by issuing a simple instruction. This will delete all data previously collected via PitchYou. Even if the applicant does not continue the communication, the data is automatically deleted 24 hours after the last message. Deletion in the company itself does not have to take place as the data is only visible to the company after successful completion.

2 Guaranteeing data security

Even though PitchYou does not send any data to WhatsApp through the WhatsApp Business API, the applicant sends their data to WhatsApp. According to WhatsApp, communication via WhatsApp itself is end-to-end encrypted. This means that only the parties involved in the communication can read the messages. WhatsApp is only notified of communication taking place ('metadata'). However, as applicants use their own private WhatsApp profile, the metadata generated is transmitted to WhatsApp and stored on servers in the US.

Their communication via the WhatsApp Business API is also end-to-end encrypted. In addition, a corresponding commissioned processing agreement was concluded with the WhatsApp Business API provider, which contractually ensures data security through appropriate technical and organisational measures. The metadata generated on the company's side is exclusively stored on the servers of the hosting partner, Hetzner Online GmbH, in Germany and is not transferred to WhatsApp.

3 Data storage and deletion

3.1 Storage period when using the PitchYou applicant tracking system

If you process personal data, the principles of the GDPR apply to you. This also includes the limitation of storage according to Article 5 (1) (e) of the GDPR. Personal data may only be stored for as long as necessary for its purposes. Therefore, the WhatsApp Business API provider immediately deletes all personal data as soon as it has been transferred to PitchYou.

If applicants are not eligible, their applications can be moved to the rejection area at any time, where applications can then be permanently deleted. The application will then no longer be visible to you.
If applicants feel discriminated against on the basis of their gender, religion, ideology, age, sexual identity, disability or ethnic origin, they have a right to take action under sentence 1 of Section 15 (4) of the General Act on Equal Treatment (Allgemeines Gleichbehandlungsgesetz, AGG). For companies to be able to defend themselves against these types of complaints, it is advisable to keep the application even after the actual rejection. As a general rule, application documents must be returned or destroyed/deleted after six months at the latest.

This maximum storage period is also adhered to when using PitchYou. If you close the application procedure and/or delete applications from the rejection area, the applications are kept in the database until the storage period expires and are then irrevocably deleted.
This ensures that application documents are not kept for longer than required.

0391 55 68 63 20 info@lgd-data.de www.lgd-data.de Rogätzer Straße 8 | 39106 Magdeburg

3.2 Storage period when connecting PitchYou to an existing applicant tracking system

If you already use an applicant management system in your company, you can easily integrate PitchYou into your existing applicant tracking system via a REST API and therefore benefit from the advantages of the WhatsApp application. Applicant data is transferred to the third-party system via an interface and deleted from PitchYou immediately after it is transferred. Further processing and deletion then takes place exclusively in the third-party system.

3.3 Storage location

Regardless of how applicants contact you, you must ensure that their data is stored or saved securely. The GDPR created strict rules for data protection to ensure high data protection standards. EU-wide application also ensures that there is an adequate level of data protection within the member countries. Under European data protection law, an adequate level of data protection does not exist outside the EU. Therefore, the GDPR restricts international data transfers. This includes storage on servers outside the EU.

As application data also often concerns sensitive data, PitchYou exclusively stores all data on servers in Germany to ensure an adequate level of data protection. The hosting partner is Hetzner Online GmbH. As one of the leading web hosting providers and an experienced data centre operator, Hetzner adheres to extensive technical and organisational measures.

The data cached by the WhatsApp Business API provider is also exclusively stored on servers in Germany, according to the provider. Transmission to WhatsApp does not take place.

However, as applicants do not communicate with the company via an API and therefore use WhatsApp directly via a smartphone, data transfer to the US takes place inherently. As WhatsApp users, applicants have already agreed to this by accepting the terms of use. Nevertheless, consent is obtained once again as part of the application process. This ensures the permissibility of data transfers after the end of the EU-US Privacy Shield. In addition, WhatsApp has responded after the ECJ ruling and now relies on standard data protection clauses concluded with the WhatsApp Business API providers.

4 Access to data

In order to protect applicant data from unauthorised access, data is saved in the PitchYou database regardless of the application channel and this is protected by a login process. This means that only authorised employees are given access to the applications.

PitchYou also works with access permissions when sharing applications within your company. By sharing the application, the recipient receives a link to the application and a PIN to open this one application. This ensures that only authorised persons have access to the data.

You can also export applications as PDFs. In this case, PitchYou cannot technically guarantee that the applicant's data will not be viewed by unauthorised employees. However, this is your responsibility and not the responsibility of PitchYou.

0391 55 68 63 20 info@lgd-data.de www.lgd-data.de Rogätzer Straße 8 | 39106 Magdeburg

5 Further notes on the GDPR-compliant use of PitchYou

Pursuant to Article 22 (1) of the GDPR, everyone has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly affects them in a significant way.

PitchYou qualifies each applicant based on the criteria you have previously set and carries out a matching assessment. However, profiling is not carried out. The matching assessment is only an indicative measure for recruiters. PitchYou does not make automated decisions such as 'reject' or 'accept'. No automated decisions ('reject' or 'accept') are made on the basis of matching. The decision as to whether an applicant is interesting or not lies with you.

If you have any further questions, please contact:

SBB Software und Beratung GmbH
Bahnhofstraße 7
95119 Naila, Germany
E-Mail: info@software-group.de
Phone: +49 9282 98410-50

or

Joelle Hirsch
LGD Datenschutz GmbH
Rogätzer Straße 8
39106 Magdeburg, Germany
E-Mail: j.hirsch@lgd-data.de
Tel.: +49 391 55686325

Joelle Hirsch
Certified Data Protection Officer
Certified Data Protection Auditor