

Statement on the data protection-compliant use of the recruiting platform "PitchYou" – English Translation – Original can be found attached

The protection of personal data is particularly important in the context of application processes. Applicants are increasingly able to contact companies online. And this is precisely where data protection plays a major role. With PitchYou, potential employees can even apply via WhatsApp.

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

With the following information, we would like to inform you that you, as a company, can integrate the recruiting application PitchYou into your application process in compliance with the GDPR.

1 General information on data protection

Personal data may only be processed in a comprehensible, i.e., transparent manner. This follows from Art. 5 (1) (a) GDPR. Therefore, applicants must be informed about the (planned) processing of their personal data in accordance with Art. 13 GDPR. Both PitchYou and you as a company fulfill this obligation by informing applicants about your privacy policies when explaining the first steps of the application process via PitchYou. However, this assumes that you have expanded your privacy policy regarding applicant data and the use of PitchYou. PitchYou provides you with a verified suggested wording for this purpose.

When using WhatsApp, the phone book and contact book are synchronized. The data is then automatically transferred to the USA. From a data protection perspective, this is problematic, as generally very few contacts consent to the transfer to WhatsApp or to third countries. Users who use WhatsApp themselves have already consented to this in the terms and conditions. Those who do not have it, however, do not.

With the WhatsApp Business API, PitchYou relies on a data protection-friendly solution, as no smartphone is required on your end within the company to communicate with applicants. Address book synchronization is therefore impossible. Therefore, no "third-party" data is transferred to WhatsApp.

Furthermore, data processing must be lawful. The legitimacy criteria are set out in Art. 6 GDPR. Before applicants can contact you via WhatsApp, consent is obtained through an opt-in process. This occurs via the homepage, which loads when the QR code is scanned or the link is opened. Applications without consent are therefore excluded.

Since the processing of personal data is based on consent, the applicant has the right to withdraw their consent at any time in accordance with Art. 7 (3) GDPR. At PitchYou, the applicant always retains full control over the 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 communication channel (e.g., online form or email).

If the applicant wishes to withdraw their application entirely, they have the option of ending the communication with a simple command. This will delete all data collected so far from PitchYou. Even if the applicant does not continue the communication, the data will be automatically deleted 24 hours after the last message. Deletion within the company itself is not necessary, as the data is only visible to the company after successful completion.

2 Ensuring data security

Even if PitchYou does not transmit any data to WhatsApp via the WhatsApp Business API, the applicant still 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 only receives the information that communication is taking place (so-called metadata). However, since applicants use their own private WhatsApp profile, the resulting metadata is transmitted to WhatsApp and stored on US servers.

Your communication via the WhatsApp Business API is also end-to-end encrypted. In addition, a corresponding data processing agreement has been concluded with the WhatsApp Business API provider, which contractually guarantees data security through appropriate technical and organizational measures. The metadata generated by the company is stored exclusively on the servers of the hosting partner, Hetzner Online GmbH, in Germany and is not transferred to WhatsApp.

3 Storage and Deletion of Data

3.1 Storage Period when Using the PitchYou Applicant Management System

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

If applicants are not considered, their applications can be moved to the rejection area at any time – applications can then be permanently deleted there. The application will then no longer be visible to you.

If applicants feel discriminated against due to their gender, religion, ideology, age, sexual identity, disability, or ethnic origin, they have the right to sue under Section 15 (4) Sentence 1 of the General Equal Treatment Act (AGG). To enable companies to defend themselves against the lawsuit, it is advisable to retain the application even after the actual rejection.

In general, application documents must be returned or destroyed/deleted within six months at the latest.

This maximum retention period is also adhered to when using PitchYou. If you complete the application process and/or delete applications from the rejection section, the applications will be retained in the database until the retention period expires and then irrevocably deleted.

This ensures that application documents are not retained longer than required.

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

If your company already uses an applicant management system, you can easily integrate PitchYou into your existing applicant management system via a REST API and thus take advantage of the benefits of WhatsApp applications. Applicant data is thus transferred to the third-party system via an interface and deleted from PitchYou immediately after transfer. Further processing and deletion then takes place exclusively in the third-party system.

3.3 Storage location

Regardless of how applicants contact you, it must be ensured that their data is stored securely. To ensure high data protection standards, the GDPR established strict data protection regulations. The EU-wide scope also ensures that an adequate level of data protection is maintained within the member states. According to European data protection law, there is no adequate level of data protection outside the EU. Therefore, the GDPR restricts international data transfers. This includes storage on servers outside the EU.

Since application data is often sensitive, PitchYou stores all data exclusively 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 center operator, Hetzner maintains extensive technical and organizational measures.

<https://www.hetzner.com/AV/TOM.pdf>

According to the provider, the data cached by the WhatsApp Business API provider is also stored exclusively on servers in Germany. No data is transferred to WhatsApp.

However, since applicants do not communicate with the company via an API and therefore use WhatsApp directly via their smartphone, a US data transfer naturally takes place. Applicants, as WhatsApp users, have already agreed to this by accepting the terms of use. However, consent is still obtained as part of the application process. This ensures the permissibility of data transfer even after the expiration of the EU-US Privacy Shield. Furthermore, WhatsApp has responded to the ECJ ruling and now relies on standard data protection clauses concluded with the WhatsApp Business API providers.

4 Data Access

To protect applicants' data from unauthorized access, data is stored in the PitchYou database regardless of the application channel and protected by a login. This means that only authorized employees have access to the applications.

PitchYou also uses 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 that specific application. This ensures that only authorized people 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 unauthorized employees. However, this is your responsibility and not PitchYou's.

5 Further information on the GDPR-compliant use of PitchYou

According to Art. 22 (1) GDPR, every person has the right to object to the processing of personal data, the right not to be subjected to a decision based solely on automated processing – including profiling – that produces legal effects concerning them or similarly significantly affects them.

PitchYou qualifies each applicant based on the criteria you previously set and makes a matching assessment. However, profiling is not carried out. The matching assessment is merely an indication for recruiters. PitchYou does not make automated decisions such as acceptance or rejection. No automated decisions (acceptance or rejection) are made based on the matching. The decision as to whether an applicant is interesting or not remains with you.

Stellungnahme zum datenschutzkonformen Einsatz der Recruiting-Plattform „PitchYou“

Der Schutz personenbezogener Daten ist gerade im Rahmen von Bewerbungsverfahren wichtig. Immer häufiger können sich Bewerber online an Unternehmen wenden. Und gerade hier spielt der Datenschutz eine große Rolle. Mit PitchYou können sich potenzielle Mitarbeiter sogar über WhatsApp bewerben.

Immer dann, wenn externe Dienstleister oder Services verwendet werden, muss die Einhaltung des Datenschutzes geprüft werden. Denn werden Bewerbungsdaten wegen mangelndem Datenschutz missbraucht, wären die Bewerber angreifbar und unter Umständen hohen Risiken wie Identitätsmissbrauch ausgesetzt.

Mit den nachfolgenden Ausführungen möchten wir Sie darüber informieren, dass Sie als Unternehmen die Recruiting-Anwendung PitchYou DSGVO-konform in Ihren Bewerbungsprozess einbinden können.

1 Allgemeines zum Datenschutz

Personenbezogene Daten dürfen nur auf eine nachvollziehbare, d. h. transparente Art und Weise verarbeitet werden. Dies ergibt sich aus Art. 5 Abs. 1 lit a DSGVO. Daher müssen Bewerber gem. Art. 13 DSGVO über die (geplante) Verarbeitung ihrer personenbezogenen Daten informiert werden. Dieser Pflicht kommen sowohl PitchYou als auch Sie als Unternehmen nach, indem Bewerber bereits bei Erläuterung der ersten Schritte des Bewerbungsverfahrens über PitchYou auf Ihre Datenschutzerklärungen hingewiesen werden. Vorausgesetzt wird aber, dass Sie Ihre Datenschutzerklärung hinsichtlich Bewerberdaten und der Verwendung von PitchYou erweitert haben. PitchYou stellt Ihnen hierfür einen geprüften Formulierungsvorschlag zur Verfügung.

Bei der Benutzung von WhatsApp erfolgt eine Synchronisation des Telefon- und Kontaktbuchs. Die Daten werden anschließend automatisch in die USA übermittelt. Aus datenschutzrechtlicher Sicht ist dies problematisch, da in der Regel die wenigsten Kontakte mit der Übermittlung an WhatsApp bzw. in Drittländer einverstanden sind. Nutzer, die selbst WhatsApp verwenden, haben in den AGB bereits darin eingewilligt. Solche, die es nicht nutzen, aber eben nicht.

PitchYou setzt mit der WhatsApp Business API auf eine datenschutzfreundliche Lösung, da zur Kommunikation mit Bewerbern kein Smartphone auf Ihrer Seite im Unternehmen notwendig ist. Ein Adressbuchabgleich ist daher ausgeschlossen. Eine Übermittlung von „fremden“ Daten an WhatsApp findet somit nicht statt.

Darüber hinaus muss die Datenverarbeitung rechtmäßig sein. Die Legitimationstatbestände stehen in Art. 6 DSGVO. Bevor sich Bewerber an Sie per WhatsApp wenden können, wird eine Einwilligung im Opt-In-Verfahren eingeholt. Dies geschieht über die Startseite, die beim Scannen des QR-Codes bzw. Öffnen des Links lädt. Eine Bewerbung ohne Einwilligung ist somit ausgeschlossen.

Da die Verarbeitung der personenbezogenen Daten auf einer Einwilligung beruht, hat der Bewerber gem. Art. 7 Abs. 3 DSGVO das Recht, jederzeit seine Einwilligung zu widerrufen. Bei PitchYou behält der Bewerber immer die volle Kontrolle über die Kommunikation und seine Daten. Sofern sich der Bewerber doch gegen die Kommunikation über WhatsApp entscheidet, kann er die Kommunikation jederzeit abbrechen und einen alternativen Kommunikationskanal (z. B. Online-Formular oder E-Mail) nutzen.

Möchte der Bewerber seine Bewerbung gänzlich zurückziehen, hat er die Möglichkeit, die Kommunikation durch einen einfachen Befehl zu beenden. Hierdurch werden alle bisher gesammelten Daten bei PitchYou gelöscht. Auch wenn der Bewerber die Kommunikation nicht weiterführt, werden die Daten 24 Stunden nach der letzten Nachricht automatisch gelöscht. Ein Löschen im Unternehmen selbst muss nicht erfolgen, da die Daten erst nach erfolgreichem Abschluss dem Unternehmen sichtbar sind.

2 Gewährleistung der Datensicherheit

Auch wenn PitchYou durch die WhatsApp Business API keine Daten an WhatsApp übermittelt, sendet der Bewerber seine Daten an WhatsApp. Die Kommunikation über WhatsApp selbst ist laut Angabe von WhatsApp Ende-zu-Ende verschlüsselt. Das bedeutet, dass lediglich die an der Kommunikation beteiligten Parteien die Nachrichten lesen können. WhatsApp erhält lediglich die Information, dass eine Kommunikation stattfindet (sog. Metadaten). Da die Bewerber jedoch ihr eigenes, privates WhatsApp-Profil nutzen, werden die anfallenden Metadaten an WhatsApp übermittelt und auf US-Servern gespeichert. Auch Ihre Kommunikation über die WhatsApp Business API ist Ende-zu-Ende verschlüsselt. Darüber hinaus wurde mit dem WhatsApp Business API-Provider ein entsprechender Auftragsverarbeitungsvertrag geschlossen, der die Datensicherheit durch geeignete technische und organisatorische Maßnahmen vertraglich zusichert. Die auf Seiten des Unternehmens anfallende Metadaten werden ausschließlich auf den Servern des Hosting-Partners, Hetzner Online GmbH, in Deutschland gespeichert und nicht an WhatsApp übertragen.

3 Speicherung und Löschung der Daten

3.1 Speicherdauer bei Nutzung des PitchYou Bewerbermanagementsystems

Verarbeiten Sie personenbezogene Daten, gelten für Sie die Grundsätze der DSGVO. Dazu zählt auch die Speicherbegrenzung gem. Art. 5 Abs. 1 lit. e DSGVO. Personenbezogene Daten dürfen nur so lange wie für die Zwecke erforderlich gespeichert werden. Daher werden beim WhatsApp Business API-Provider sämtliche personenbezogene Daten sofort gelöscht, sobald sie an PitchYou übertragen wurden.

Kommen Bewerber nicht in Frage, können ihre Bewerbungen jederzeit in den Absagenbereich geschoben werden – dort können Bewerbungen nun endgültig gelöscht werden. Für Sie ist die Bewerbung dann nicht mehr sichtbar.

Fühlen sich Bewerber aufgrund ihres Geschlechts, ihrer Religion, Weltanschauung, des Alters, sexuellen Identität, Behinderung oder ethnischer Herkunft benachteiligt, steht ihnen nach § 15 Abs. 4 S. 1 AGG ein Klagerecht zu. Damit sich Unternehmen gegen die Klage verteidigen können, ist es ratsam, die Bewerbung auch über die eigentliche Absage hinaus aufzubewahren.

Allgemein gilt, dass Bewerbungsunterlagen spätestens nach sechs Monaten zurückgegeben bzw. vernichtet/gelöscht werden müssen.

An diese maximale Aufbewahrungsfrist wird sich auch beim Einsatz von PitchYou gehalten. Schließen Sie das Bewerbungsverfahren ab und/oder löschen Bewerbungen aus dem Absagenbereich, werden die Bewerbungen in der Datenbank bis zum Ablauf der Aufbewahrungsfrist aufbewahrt und anschließend unwiderruflich gelöscht.

Dadurch ist gewährleistet, dass Bewerbungsunterlagen nicht länger als vorgeschrieben aufbewahrt werden.

3.2 Speicherdauer bei Anbindung von PitchYou an ein bestehendes Bewerbermanagementsystem

Nutzen Sie im Unternehmen bereits ein Bewerbermanagementsystem, können Sie PitchYou ganz einfach über eine REST-API in Ihr bestehendes Bewerbermanagementsystem integrieren und so die Vorteile der WhatsApp-Bewerbung nutzen. Bewerberdaten werden somit über eine Schnittstelle in das Drittsystem übertragen und unmittelbar nach Übertragung bei PitchYou gelöscht. Die weitere Verarbeitung und Löschung erfolgt dann ausschließlich im Drittsystem.

3.3 Speicherort

Unabhängig davon, auf welchem Wege sich Bewerber bei Ihnen melden, muss gewährleistet sein, dass ihre Daten sicher aufbewahrt bzw. gespeichert werden. Um hohe Datenschutz-Standards zu gewährleisten, wurden mit der DSGVO strenge Regeln für den Datenschutz geschaffen. Durch die EU-weite Geltung wird zudem gewährleistet, dass ein angemessenes Datenschutzniveau innerhalb der Mitgliedsländer vorhanden ist. Nach europäischem Datenschutzrecht besteht außerhalb der EU kein angemessenes Datenschutzniveau. Daher schränkt die DSGVO die internationale Datenübermittlung ein. Dazu zählt auch die Speicherung auf Servern außerhalb der EU.

Da es sich bei Bewerbungsdaten regelmäßig auch um sensible Daten handelt, speichert PitchYou alle Daten ausschließlich auf Servern in Deutschland, um ein angemessenes Datenschutzniveau zu gewährleisten. Hosting-Partner ist die Hetzner Online GmbH. Als einer der führenden Webhosting-Anbieter und erfahrener Rechenzentrumsbetreiber hält Hetzner umfangreiche technische und organisatorische Maßnahmen¹ ein.

¹ <https://www.hetzner.com/AV/TOM.pdf>

Auch die beim WhatsApp Business API-Provider zwischengespeicherten Daten werden nach Angaben des Providers ausschließlich auf Servern in Deutschland gespeichert. Eine Übermittlung an WhatsApp findet nicht statt.

Da die Bewerber jedoch nicht über eine API mit dem Unternehmen kommunizieren und daher WhatsApp direkt über das Smartphone verwenden, findet naturgemäß ein US-Datentransfer statt. Diesem haben die Bewerber als Nutzer von WhatsApp mit Akzeptieren der Nutzungsbedingungen bereits zugestimmt. Dennoch wird nochmals im Rahmen der Bewerbung eine Einwilligung eingeholt. So ist auch nach dem Ende des EU-US Privacy Shields die Zulässigkeit der Datenübermittlung gewährleistet. Zudem hat WhatsApp nach der EuGH-Entscheidung reagiert und setzt nun auf Standarddatenschutzklauseln, die mit den WhatsApp Business API-Providern geschlossen wurden.

4 Zugriff auf Daten

Um die Daten der Bewerber vor unberechtigtem Zugriff zu schützen, werden Daten unabhängig des Bewerbungskanal in der Datenbank von PitchYou gespeichert und per Login geschützt. Das bedeutet, dass nur berechtigte Mitarbeiter Einsicht in die Bewerbungen erhalten.

Auch bei der Weitergabe von Bewerbungen innerhalb Ihres Unternehmens arbeitet PitchYou mit Zugriffsberechtigungen. Durch Teilen der Bewerbung erhält der Empfänger einen Link zur Bewerbung und zusätzlich eine PIN zum Öffnen dieser einen Bewerbung. Dadurch ist gewährleistet, dass bei Ihnen nur diejenigen Personen Zugriff auf die Daten haben, die dazu berechtigt sind.

Sie können die Bewerbungen ebenfalls per PDF exportieren. In diesem Fall kann PitchYou technisch nicht gewährleisten, dass die Daten des Bewerbers nicht durch unberechtigte Mitarbeiter eingesehen werden. Dies liegt jedoch in Ihrer Verantwortung und nicht bei PitchYou.

5 Weitere Hinweise zur DSGVO-konformen Verwendung von PitchYou

Jede Person hat gem. Art. 22 Abs. 1 DSGVO das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

PitchYou qualifiziert jeden Bewerber anhand der vorher von Ihnen eingestellten Kriterien und trifft eine Matching-Einschätzung. Ein Profiling wird jedoch nicht durchgeführt. Die Matching-Einschätzung ist lediglich ein Hinweis für Recruiter. Automatisierte Entscheidungen wie Ab- oder Zusagen werden durch PitchYou nicht getroffen. Es erfolgen keine automatisierten Entscheidungen (Ab- oder Zusagen) auf Grundlage des Matchings. Die Entscheidung, ob ein Bewerber interessant ist oder nicht, bleibt bei Ihnen.

Bei weiteren Fragen wenden Sie sich an:

Joelle Hirsch
LGD Datenschutz GmbH
Rogätzer Straße 8
39106 Magdeburg
E-Mail: j.hirsch@lgd-data.de
Tel.: 0391 55686325

LGD Datenschutz GmbH info@lgd-data.de www.lgd-data.de	LGD Datenschutz GmbH Rogätzer Straße 8 39106 Magdeburg +49 391 55686322 +49 391 55686327
--	---

Joelle Hirsch
Zertifizierte Datenschutzbeauftragte
Zertifizierte Datenschutzauditorin

