

Poznaj Privacy Policy

Effective from: 3 October 2026

This Privacy Policy describes what personal data is processed in connection with the use of the Poznaj app, for what purposes, on what legal basis, to whom it is disclosed and for how long it is kept. Data is processed solely to the extent necessary to provide the Services described in the Terms of Service.

This is a translation of the Polish original for information purposes. In case of any discrepancy, the Polish version prevails.

§ 1. Data controller

1. The controller of personal data is Sebastian Zabrzyski, conducting business activity under the name BitPerfect Sebastian Zabrzyski, address for correspondence: ul. Grunwaldzka 8A/15, 39-300 Mielec, Poland, VAT ID (NIP) 5862377082, statistical ID (REGON) 521142580, entered in the Central Register and Information on Business Activity (CEIDG).
2. In all matters concerning personal data protection, including to exercise the rights described in § 9, the Controller may be contacted at kontakt@poznaj.pl, through the contact form in the App, or by post at the address given in paragraph 1.

§ 2. What this policy is

1. This policy describes how the personal data of people using the Poznaj mobile app and its supporting servers is processed, as well as the rules on accessing data on the User's device.
 2. Capitalised terms have the meaning given to them in the Poznaj Terms of Service.
 3. Data is processed in accordance with the GDPR and, in matters not governed by the GDPR, in accordance with the Polish Act of 10 May 2018 on the protection of personal data and the Act on Providing Services by Electronic Means.
-

§ 3. Categories of data processed

The Controller processes the following categories of data:

- **Registration and authentication data** — e-mail address, password stored solely as an irreversible hash, the identifier of the account held with an Identity provider together with the e-mail address it supplied, first name, date of birth used to confirm that the User is at least 18 and to calculate the age shown to others, gender, town selected from a list, the selected App language, and data on the state of the Account, including the date it was created and the date of last activity.
- **Profile data** — profile photos together with their verification status, the description, selected interests, information about openness to meeting people for dating purposes, the Profile visibility setting and information about any restriction of the Account.
- **Data on activity in the App** — Meetups created by the User together with their place, time and description, participation in other people's Meetups and

its status, invitations and waves sent and received, votes cast in Polls, the list of blocked Users, muted conversations and notification settings, including quiet hours.

- **Content created by the User** — text messages, photos and voice recordings sent via the Chat, Polls created in Meetups and the content of moderation reports submitted.
- **Location data** — to the extent described in § 5: the approximate position of Presence together with an optional message and the time until which it is to be visible, the approximate last position of the device used to calculate distance, and the Meetup place indicated by the Organiser.
- **Data on the devices the User is signed in on** — operating system, device name, App version, push notification token and the date of last use.
- **Technical and evidential data** — the IP address and the date and time of acceptance of the Terms and of the confirmation that this policy has been read, the versions of these documents the User has read on registration and in notices of their changes, together with the date and time of confirmation, kept in order to demonstrate compliance with the accountability obligation under Article 5(2) GDPR, as well as standard server logs and technical diagnostic data submitted when errors occur.
- **Moderation data** — reports submitted by the User and reports concerning the User, together with their content and outcome, information about the measures applied, and the log of administrative actions together with the ground and the statement of reasons provided under Article 17 of the Digital Services Act.

- **System notifications** — the history of notifications about events concerning the Account, together with information on whether they have been read.

Accounts created through an Identity provider. When an Account is created, or a sign-in is made, through Google or Facebook, the Controller receives from that provider the identifier of the User's account with it, their first name and — where the provider makes it available — their e-mail address. The Controller receives neither the password to the User's account with the provider nor access to any of its other services.

§ 4. Purposes and legal bases of processing

The retention periods for all of the purposes below are set out in § 8.

Creating and maintaining the Account and providing the Services — organising and joining Meetups, the People directory, the Map, the Chat:

- data: registration and authentication data, Profile data, data on activity in the App, content created by the User,
- basis: Article 6(1)(b) GDPR — processing necessary for the performance of a contract to which the data subject is party and in order to take steps prior to entering into it.

Calculating the distance shown in the People directory and in the list of Meetups:

- data: the approximate last position of the device together with information about its source and the date it was updated,

- basis: Article 6(1)(b) GDPR — the feature forms part of the People directory and the list of Meetups described in the Terms; its use depends solely on granting and maintaining the location permission in the operating system, and withdrawing that permission immediately stops the collection of new readings.

Publication of the User's image in the Profile, together with review of the photo before publication:

- data: profile photos together with their verification status and the result of the automated preliminary classification of the photo (§ 12(4)),
- basis: Article 6(1)(b) GDPR — a profile photo is a required element of the Profile (§ 5(5) and § 6 of the Terms), and the User grants permission to disseminate their image on the terms set out in § 6(5) of the Terms; as regards the review of the photo before publication — Article 6(1)(f) GDPR, the legitimate interest of protecting Users against an untrue or inappropriate image in another person's Profile.

Securing access to the Account — verification and change of the e-mail address, setting and resetting the password, handling device sessions:

- data: the e-mail address — the current one and, where it is being changed, the new one until the change is confirmed — verification tokens and device data,
- basis: Article 6(1)(b) GDPR and Article 6(1)(f) GDPR — the legitimate interest of securing access to the Account. A change of address requires confirmation with the password or, for an Account without a password, confirmation through the Identity provider, and takes effect only once the link sent to the new address is clicked; the previous address is also informed of the change

request.

Push and e-mail notifications and messages shown in the open App about events concerning the Account and Meetups, and their history in the App:

- data: e-mail address, push notification token, notification settings, system notifications,
- basis: Article 6(1)(b) GDPR — notifications form part of the Service.

Notifications about messages, waves, invitations and Polls and about events in Meetups — a Participant joining or withdrawing, a request to join or to confirm attendance, a place becoming available, an upcoming start, and a change to or cancellation of a Meetup — can be switched off by type in the App's settings and muted for a selected conversation or Meetup.

Notifications of decisions concerning the User themselves — the acceptance or rejection of their request to join, their removal from a Meetup, the cancellation of a Meetup by the administration, the outcome of photo review, the receipt and handling of a report, the removal of a message, the imposition and lifting of a restriction on the Account, and its suspension and reinstatement — cannot be switched off, as they serve to inform the User of a decision that concerns them. During the quiet hours set, push notifications are not sent.

Security, content moderation and prevention of abuse — handling reports, blocking, rate limiting, detecting abuse:

- data: moderation data, reported content, IP address,
- basis: Article 6(1)(f) GDPR — the legitimate interest of ensuring Users' safety and the integrity of the App and, as regards obligations arising from the Digital Services Act, also Article 6(1)(c) GDPR.

Demonstrating acceptance of the Terms, that this policy has been read and that the User was informed of changes to them:

- data: IP address and the date and time of acceptance and confirmation, as well as the versions of the documents the User has read, together with the date and time of confirmation,
- basis: Article 6(1)(f) GDPR — the legitimate interest of demonstrating that the agreement was concluded on the terms of the Terms, that the User was informed of changes to them and that the information obligation was fulfilled (Article 5(2) GDPR).

Keeping the App technically operational and diagnosing failures:

- data: server logs covering the IP address, the date of the request, the full request address together with its parameters and the header identifying the client software (User-Agent), as well as technical diagnostic data from the device — device model, system and App version, the error message, the request address at which the error occurred and the actions immediately preceding it (for example requests made and interface elements tapped), and, for some sessions, App performance measurements,
- basis: Article 6(1)(f) GDPR — the legitimate interest of ensuring the proper operation of the service.

Handling correspondence sent to the Controller by e-mail or through the contact form in the App:

- data: the sender's e-mail address or the reply address provided in the form, the content of the message and, for the form, also the selected subject and — where the message is sent from a signed-in Account — its identifier and

first name,

- basis: Article 6(1)(f) GDPR — the legitimate interest of replying to the message and, as regards complaints and obligations arising from the Digital Services Act and the GDPR, Article 6(1)(c) GDPR. Messages from the form are not saved in the App's database — they go solely to the Controller's mailbox; only a message that could not be delivered remains in the system until delivery is retried or the message is deleted.

Establishing, pursuing and defending claims:

- data: e-mail address, first name, IP address, correspondence and the data necessary in the particular case,
- basis: Article 6(1)(f) GDPR — the legitimate interest of pursuing claims and defending against them.

Compliance with legal obligations, in particular responding to authorised authorities:

- data: the data necessary to the extent resulting from the authority's request,
- basis: Article 6(1)(c) GDPR.

§ 5. Location

1. The App uses the device's location only where the permission has been granted in the operating system and only for the features that require it: displaying the Map, indicating Presence, calculating the distance and the search radius in the list of Meetups and in the People directory, and pre-setting the place when a Meetup is created. Refusing the permission does not block the App's remaining features

— the distance is then calculated from the town indicated in the Profile and, after the permission is withdrawn, from the last stored approximate position until it is replaced as set out in § 8.

2. Exact coordinates are processed solely for the time needed to handle the request, in order to calculate the approximate position or the distance, and are not saved in the database. Only an approximate position is stored, offset from the real one in a way that makes the real one impossible to reconstruct, and the distance shown to other Users is additionally rounded. The request address together with its parameters may, however, be recorded for a short time in the server logs and sent to the providers monitoring errors and the App's operation (§ 7).

3. The App does not track location in the background. The device's position is read only while the App is open and active in the foreground; this also applies to the renewal of Presence.

4. The Meetup place is stored exactly, since its purpose is to let the Organiser indicate the meeting point to Participants.

§ 6. What data is visible in the App

1. Persons who are not logged in (Guests) can see the Profile data together with approved photos, the trace of last activity, the approximate distance calculated as described in § 5, the date of joining the App and the User's upcoming Meetups where the User is their Organiser. Indicated Presence is visible to Guests on the Map together with the first name, age and main photo, but without the message attached to it.

2. Profile visibility to Guests can be switched off in the App's settings; the Profile and Presence then remain visible only to logged-in Users. This does not apply to the Organiser's data presented with their Meetups (paragraph 8).

3. Logged-in Users can additionally see the message attached to Presence and the interests they have in common. Only a logged-in User can message another User and invite them to a Meetup.

4. A photo awaiting review is not visible to anyone other than its owner and the persons reviewing photos on the Controller's side — until it is approved, other people see a default placeholder.

5. Only the Account holder sees their e-mail address, exact date of birth, selected App language, Profile visibility setting and information about any restriction of the Account. This data is not made available to anyone else, other than persons on the Controller's side for whom access is necessary to review photos and handle reports (§ 14(5)).

6. The content of Chat conversations is available only to their participants. The Controller does not read it in the ordinary course of its activity — it does so only at the request of an authorised authority or in connection with a moderation report. In the latter case, access covers the conversation the report concerns, including the earlier messages needed to assess the context, and is recorded in the log of administrative actions. The automated check of a photo before it is sent, described in § 12(5), takes place without human involvement. In addition, the sender's first name and the content of a new text message are included in the push notification delivered by the entities indicated in § 7(1).

7. A Meetup's Polls — the question, the answers and the voting result — are visible only to the Organiser and the Participants of that Meetup. The result is

attributed: the first names of the people who chose each answer are shown.

8. Meetups — their name, description, place and time — are also visible to Guests, together with the Organiser's Profile data, including their first name, age and profile photo, even where the Organiser has switched off Profile visibility to Guests.

9. The list of a Meetup's Participants, together with their Profile data, is visible to every logged-in User who opens that Meetup. Answers to a request to confirm attendance are visible only to the Organiser and the Participants.

§ 7. Data recipients

1. Data is disclosed only to the following entities and only to the extent necessary for the purposes indicated:

- **Webdock.io ApS**, Asperup, Denmark — hosting of the App's servers and e-mail handling. The entity processes all data stored by the App; the data remains within the European Economic Area.
- **650 Industries, Inc. (Expo)**, United States — delivery of push notifications and distribution of App updates. The entity receives the push notification token, the content of the notification — which, for a new Chat message, includes the sender's first name and the content of the text message — and the device's IP address and, when checking for updates, also the App version, the type of operating system and a random installation identifier.
- **Functional Software, Inc. (Sentry)**, United States — error monitoring for the App and the server; the data is stored in that entity's data centre within the European Union. The entity receives technical diagnostic data together

with the device's IP address and the address of the request at which the error occurred, including its parameters (§ 5(2)). Message content and photos are not transferred to it.

- **Laravel Holdings Inc. (Laravel Nightwatch)**, New York, United States — monitoring of the App's and the server's operation. The entity receives technical data about handled requests (the method, the request address together with its parameters, the route, the handling time and the response code, and headers with authentication data omitted), the device's IP address, the identifier of the logged-in User, information about exceptions, database queries as templates without substituted values, background jobs, information about e-mails sent (the subject and the number of recipients, without their addresses or content) and server log entries. Together with the identifier of the logged-in User, the entity receives their e-mail address. Message content, photos and the contents of submitted forms are not transferred to it.
- **komoot GmbH (Photon)**, Potsdam, Germany — place search while a Meetup is being created. The query is sent by the Controller's server, so the entity receives only the search term, without data identifying the User and without the IP address of their device.
- **OpenFreeMap** (tiles.openfreemap.org) — map tiles downloaded directly by the User's device. The entity receives the device's IP address and information about the portion of the map being viewed, without data identifying the User.
- **Apple Inc.** and **Google LLC** — distribution of the App through the App Store and Google Play and delivery of push notifications, together with their content, to the device's operating system. These entities process data under

their own privacy policies, over which the Controller has no influence.

- **Google Ireland Limited**, Ireland — handling of sign-in with Google.

Authentication takes place directly between the User's device and Google; the Controller's server verifies the identity token received from the App on its own, using Google's public keys, without passing it to Google, and reads from it the data described in § 3. Google processes sign-in data as an independent controller, under its own privacy policy, over which the Controller has no influence.

- **Meta Platforms Ireland Limited**, Ireland — handling of sign-in with Facebook. The Controller's server passes the access token received from the App to Meta solely to verify its validity and to retrieve the data described in § 3. The Facebook library built into the App starts only when the User signs in with Facebook or confirms their identity with it, and then connects to Meta's servers, which receive the device's IP address and basic technical data about the App and the device; the collection of App usage events and of the device advertising identifier has been switched off in it. Meta also processes that data as an independent controller, under its own privacy policy, over which the Controller has no influence.

2. Data may additionally be disclosed to state authorities entitled to request it under the law, in particular the courts, the prosecution service and the police, solely to the extent and in the manner resulting from those provisions.

3. Personal data is not sold and is not made available to data brokers, advertising networks or providers of marketing analytics. The App contains no advertising and no tracking tools for marketing purposes.

§ 8. Retention periods

1. Data is kept no longer than is necessary for the purposes set out in § 4. The retention periods are as follows:

- Account and Profile data, data on activity in the App and content created by the User — until the Account is deleted, unless a shorter period is indicated below; the effect of deleting the Account on messages sent is described in paragraph 2,
- a profile photo that was declined or removed in moderation — deleted without delay,
- Accounts with an unconfirmed e-mail address — deleted automatically, together with all data entered, if the address is not confirmed within 7 days of registration,
- Meetups together with their Participants' conversations and Polls — deleted automatically 60 days after the start date, and Meetups organised by the User — also when their Account is deleted,
- the Presence record — ceases to be visible to other Users immediately upon expiry, and the record itself is removed from the database within a day,
- the last position used to calculate distance — replaced with the coordinates of the town indicated in the Profile if it is not updated for 7 days; deleted in full together with the Account,
- photos and voice recordings sent via the Chat — deleted automatically 7 days after being sent; attachments from a conversation to which an unexamined moderation report relates are kept until the report is examined,

- a private conversation in which none of the participants holds an Account any longer — deleted together with its messages within a day of the last of those Accounts being deleted,
- invitations — deleted once they expire, that is once the Meetup ends,
- waves — deleted automatically 30 days after the most recent wave,
- moderation reports — for 12 months after they are examined, and unexamined reports until they are examined; a report submitted by a person who has deleted their Account is kept, but no longer identifies who submitted it; reports concerning a deleted Account, a deleted Meetup, a message in such a Meetup's conversation or in a deleted private conversation are deleted together with them,
- the log of administrative actions — for 12 months from the entry, and an entry on the suspension of an Account — no shorter than the suspension lasts,
- system notifications — for 90 days after they were read and, for unread notifications, for 365 days after they arose,
- application logs on the server — for 14 days; web server access logs and technical diagnostic data held by the monitoring providers — for a short period determined by diagnostic and security needs,
- the file containing a copy of the data prepared for download (§ 9(3)) — deleted automatically within 2 hours of being prepared,
- the periodic summary of the effectiveness of automated photo classification — indefinitely; it contains only figures and photo identifiers, without the photos themselves and without their owners' data, and serves to verify that the classification thresholds remain correct,

- correspondence sent to the Controller — for the time needed to deal with the matter, no longer than the expiry of the limitation period for claims,
- data necessary to establish, pursue and defend claims — until the limitation period for claims expires.

2. After the Account is deleted, messages sent by the User remain visible to the other participants of the conversations, but are permanently detached from the Account and no longer identify its author — except for the conversations of Meetups organised by the User, which disappear together with those Meetups; the photos and recordings attached to them disappear on the ordinary schedule set out in paragraph 1. The reasoning behind this is set out in § 16(4) of the Terms.

§ 9. Rights of the data subject

1. In connection with the processing of data, the User has the right to:

- access the data and obtain a copy of it (Article 15 GDPR),
- rectify inaccurate data and complete incomplete data (Article 16 GDPR),
- erase the data, that is the so-called right to be forgotten (Article 17 GDPR),
- restrict processing (Article 18 GDPR),
- data portability for data processed on the basis of a contract, in a structured, commonly used, machine-readable format (Article 20 GDPR),
- object to processing based on a legitimate interest (Article 21 GDPR).

2. Some of these rights can be exercised directly in the App: access to one's own data and its rectification in the Profile, deletion of photos when editing the Profile,

and erasure of all data by deleting the Account in the App's settings. The first name, gender and date of birth cannot be changed by the User — their change may be requested at kontakt@poznaj.pl.

3. A copy of the data is downloaded by the User in the App's settings, without contacting the Controller. It contains, in a machine-readable format, the Account and Profile data, Meetups created by the User and their participation in other Meetups, votes in Polls, waves, invitations sent and received, the list of blocked Users, messages sent, reports submitted, signed-in devices, notification settings, the position, Presence and notification history, as well as the profile photo files in the form stored by the App and the photos and recordings the User sent via the Chat, provided the deadline for deleting them (§ 8) has not yet passed. It does not include messages or attachments received from other people — that data belongs to their authors. Access to the remaining data processed, including data not covered by the copy downloaded in the App, is provided by the Controller upon a request made under paragraph 4.

4. Other requests should be sent to kontakt@poznaj.pl. Where a request indicates a different data format, it will be used where possible.

5. The Controller provides information on the action taken in response to a request within one month of receiving it. That period may be extended by two further months where the request is complex or where a number of requests have been received; the Controller informs the data subject of any extension and of its reasons.

6. Notwithstanding a request for erasure, the Controller may continue to process data in order to establish, pursue or defend claims or to comply with a legal obligation, of which it informs the data subject.

7. A person who considers that their data is being processed unlawfully has the right to lodge a complaint with a supervisory authority. In Poland this is the President of the Personal Data Protection Office, ul. Moniuszki 1A, 00-014 Warsaw, <https://uodo.gov.pl>. A complaint may also be lodged in the Member State of habitual residence, place of work or place of the alleged infringement.

§ 10. Transfers outside the European Economic Area

1. The App's core infrastructure — servers and e-mail — is located within the European Economic Area.
 2. The only data transferred to a third country is the data indicated in § 7(1) for the entities established in the United States, that is the push notification token and content — including the sender's first name and the content of a new text message — the data related to distributing updates, the technical diagnostic data, and the data about handled requests together with the request address and the identifier and e-mail address of the logged-in User.
 3. Transfers take place on the basis of standard contractual clauses approved by the European Commission under Article 46(2)(c) GDPR and, to the extent that a given recipient participates in the EU-U.S. Data Privacy Framework, on the basis of the European Commission's adequacy decision.
 4. A copy of the relevant safeguards can be obtained by writing to kontakt@poznaj.pl.
-

§ 11. Whether providing data is voluntary

1. Providing data is voluntary; however, providing the registration data indicated in § 5(5) of the Terms is a condition of creating an Account and using the Service for registered Users. Without it, that Service cannot be provided.
 2. Providing any other data — the Profile description, additional photos, interests, information about openness to meeting people for dating purposes, Presence on the Map and the content sent via the Chat — is entirely voluntary.
 3. Using the App as a Guest requires no data at all.
 4. Signing in through an Identity provider is an alternative to registering with an e-mail address and a password, not a condition of it.
-

§ 12. Automated decision-making and profiling

1. No decisions based solely on automated processing are taken in respect of Users which would produce legal effects concerning them or similarly significantly affect them.
2. Profiling is not used. The App does not build a behavioural profile of the User, does not assess their personal characteristics and does not select people using a matching algorithm. Lists of Meetups and of people are sorted solely according to the criterion chosen by the User — distance, start time, last activity or date added.
3. Moderation decisions, including the removal of content and the suspension or deletion of an Account, are taken by a human being. The only exception is the refusal to accept a photo sent via the Chat, described in paragraph 5.

4. Before a profile photo is published, an automated preliminary classification is carried out to check it against the content prohibited by the Terms. It takes place on the Controller's server — the photo is not transferred to third parties — and does not serve to recognise identity or determine the characteristics of the persons depicted. Its only possible effect is the publication of a photo whose publication the User has themselves requested; photos about which the tool raises concerns, and those that could not be checked, are assessed by a human being. It is therefore not a decision within the meaning of paragraph 1.

5. The same tool, on the same technical basis, checks a photo sent via the Chat before it appears in the conversation. Here the tool may refuse to accept the photo on its own. The only effect of that refusal is that this single file is not sent: the photo is neither published nor stored anywhere, the Account remains unaffected, no breach is recorded, and the User may send a different photo or use the other message types. The refusal therefore produces no legal effects concerning the User and does not similarly significantly affect them, and is not a decision within the meaning of paragraph 1. The User receives the statement of reasons for the refusal, together with information that automated means were used and about the possibility of filing a complaint, immediately, in the App (§ 11(4) of the Terms).

6. Voice recordings and text messages are not checked automatically.

§ 13. Cookies and access to device storage

1. The mobile app does not use cookies within the meaning of telecommunications law.

2. The App stores data in the device's memory to the extent necessary for it to work: the access token maintaining the sign-in session, together with basic Account data, in the operating system's secure storage, selected settings and view preferences, including filters and the selected Presence mode, and a cache of displayed data, downloaded photos and recordings that speeds the App up on a poor connection.

3. Apart from location (§ 5), the App asks for permission to display notifications, for access to the camera — when taking a profile photo or a photo to be sent via the Chat — and for access to the microphone, solely for the duration of recording a voice message. A photo from the gallery is chosen by the User in the system picker, which passes only the selected photo to the App, without access to the whole gallery. Each of these permissions is granted in the operating system and may be withdrawn at any time; refusing one disables that single feature only. The App does not record audio outside the moment the User starts recording themselves, and does not take photos without their involvement.

4. This data is not shared with third parties. Signing out clears the cache of data, photos and recordings, and uninstalling the App removes all data stored on the device.

§ 14. Security

1. Passwords are stored solely as an irreversible hash, using an algorithm designed for secure password storage. The Controller does not know the User's password and is unable to reconstruct it.

2. All communication between the App and the server is encrypted.

3. Photos are not available at fixed, guessable addresses. Every request for a photo is checked on the server side and results in a signed link with a short validity period. A profile photo awaiting review requires signing in as its owner or as a person reviewing photos, and Chat photos and recordings require signing in as a participant of the conversation; an approved profile photo, like any element of a publicly visible Profile, is also available to persons who are not logged in.
 4. Signing in uses individual access tokens assigned to a specific device. The App's settings allow the list of signed-in devices to be reviewed and access from any of them to be revoked at any time; resetting the password revokes access from all devices at once.
 5. Access to data on the Controller's side is limited to persons for whom it is necessary, and solely to the extent resulting from the purpose of the processing.
 6. Despite the safeguards applied, transmitting data over the Internet is never entirely free of risk. Using a unique password and up-to-date system software on the device is recommended.
-

§ 15. Age restrictions

1. The App is intended solely for adults. Data of persons under 18 is not knowingly collected.
2. Should information be obtained that an Account has been created by a minor, that Account is deleted together with all of its data. A suspicion that such an Account exists can be reported in the App or to kontakt@poznaj.pl.

§ 16. Changes to this policy

1. This policy may change, in particular where the scope of the data processed changes, where new App features are added, where subprocessors change or where the law changes.
2. Users are informed of any changes by a notice displayed in the App, which indicates the documents changed and the day the changes take effect. The notice is made available in the App before that day.
3. This policy applies from 3 October 2026.

BitPerfect Sebastian Zabrzyski, address for correspondence: ul. Grunwaldzka 8A/15, 39-300 Mielec, Poland · kontakt@poznaj.pl