PRIVACY NOTICE

1 January 2026

Dear customers, business partners, visitors, users of information systems or applications, protection of Personal Data is very important to us and therefore we proceed in accordance with applicable legal regulations when ensuring the protection of Personal Data. Below you can find all details pertaining to processing of personal data by Zentiva.

1. Who is responsible for your Personal Data

We Zentiva Pharma UK Ltd, a legal entity which is a part of Zentiva group of companies, with its registered seat at 12 New Feter Lane, London, EC4A 1JP ID no.: 02148996 (hereinafter referred to as the **"Company")**, as a Controller, together with the other legal entities (hereinafter collectively referred to as "**Zentiva**" and/or "**we**" and/or the "**Affiliates**"), as joint controllers, would like to inform you in accordance with the UK GDPR, as incorporated into UK law by the Data Protection Act 2018, concerning the protection of natural persons with regard to the processing of personal data and the free movement of such data. (hereinafter referred to as the "**GDPR"**) on how we process your Personal Data.

2. What Personal Data do we process and how

We collect and process Personal Data in physical and/or electronic form, using both manual and automated means, strictly in line with applicable data protection laws and this Privacy Notice. As a general rule, we only process Personal Data that is adequate, relevant and limited to what is necessary for our activities and our relationship with you.

We may process the following categories of Personal Data as applicable to individual processes where they are needed:

- **Identification data**

Such as first name, surname, initials, date of birth, national/ID number, tax identification number, professional ID (where applicable), driving licence details, work and residence permit number (where applicable).

- **Contact details**

Such as postal and billing address, e-mail address (personal and/or professional), telephone number (personal and/or professional), emergency contact details of a close person.

- **Online identifiers and technical data**

Such as IP address, browser type, language settings, access times and sessions and similar data generated by your use of our website and online services (for details, see our cookie policy).

- **Professional and role-related data**

Such as workplace, profession, function, job title, department, field of activity, specialty, professional or academic degree, qualification and information on whether you are a Healthcare Professional or a representative of a legal entity.

- **Communication content and signatures**

Such as the content of your communications with us (physical and/or electronic), your questions, requests, claims, complaints or reports, as well as your physical or electronic signature and, where applicable, audio recordings (e.g. hotline calls, testimonials).

- **Recruitment and HR-related data**

Such as data on the position, department or location you apply for, information on your education, training and professional experience and other information you choose to include in your CV and/or cover letter. We

do not require other data (such as photos, copies of IDs or diplomas, criminal record or health data) unless expressly requested and justified by law.

- **Contract and transaction data**

Such as information needed to enter into and perform contracts with you (e.g. identification and contact details, tax or national ID, contractual relationship details, documents and evidence relating to performance of the contract) and data relating to the purchase or sale of goods (e.g. goods description, related correspondence and signatures).

- **Product safety, quality and pharmacovigilance data**

In connection with adverse event reports or product quality complaints, we may process data relating to:

- the reporter or claimant (identification and contact details, qualification/role, content of the report);
- the person who experienced the adverse event (initials, date of birth, age/age category, gender, pregnancy period where applicable);
- description of the adverse event or quality complaint (signs and symptoms, date of occurrence, outcome, description of the quality issue);
- information on the concerned product.

- **Visitor and site security data**

For visitors to our premises, we may process identification data (name, surname, basic ID details read only, vehicle registration number without automatic recognition), workplace and title, time of arrival and departure, destination within our premises, data resulting from internal training questionnaires, general health screening data where required (e.g. temperature, symptoms or exposure related to infectious diseases such as COVID-19), image (e.g. security or access photos, without facial recognition) and electronic or holographic signature.

- **Vehicle, accident and insurance data**

In connection with traffic accidents involving vehicles owned or used by us, we may process data about drivers, vehicle owners and eyewitnesses, such as identification and contact details, accident details (date, place, circumstances, accident sketch), vehicle characteristics (make, type, registration number, country of registration) and insurance details (insurer, policy number and validity, coverage), as well as related communications and signatures.

- **Whistleblowing and compliance data**

Where you are involved in whistleblowing reports (as whistle-blower, alleged wrongdoer, witness or other third party), we may process identification and contact details, work and residence permit number (if applicable), information on disciplinary measures/actions, and the content of the report and related communications.

- **Event and marketing communication data**

If you subscribe to our newsletters or participate in events organised or attended by us, we may process your identification and contact details, workplace and title (where relevant), consent-related information (e.g. grant or withdrawal of consent), as well as visual and audio recordings (photos, videos, voice recordings) from the events. Such materials may be shared via our internal and/or external communication channels (e.g. website, social media, internal platforms), in accordance with applicable law.

- **Social media content**

In connection with our social media presence (e.g. LinkedIn), we may process data such as your username, profile picture and status, as well as reactions, comments, shares and similar interactions with our content or with content we interact with, based on our legitimate interests and as described in this Privacy Notice.

- **Special categories of Personal Data**

We do not intentionally collect special categories of Personal Data (such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric data, health data, or data concerning sex life or sexual orientation) ("Sensitive Personal Data"). We may process certain health-related data or similar information only in strictly limited circumstances provided by law (for example, in the context of pharmacovigilance, product safety and quality, or health and safety requirements at our premises), subject to appropriate safeguards.

If you do not provide the Personal Data we request, we may not be able to perform the activities described in this Privacy Notice or to comply with our legal and/or contractual obligations.

3. How do we obtain your Personal Data

We obtain your Personal Data directly from you. We may also collect certain Personal Data automatically when you visit our website (for details, please see our cookie policy: https://www.zentiva.com/cookie-policy.

We may further obtain your Personal Data from other sources, including:

- other legal entities within the Zentiva group;
- other public or private entities, with or without legal personality (for example your employer, our business partners, or central and local public authorities acting within their legal powers, including supervisory and investigative authorities);
- in connection with mergers, acquisitions, transfers of assets or assignments of receivables;
- other individuals (for example persons reporting side effects you experienced, or individuals involved in traffic accidents who are not the owner of the vehicle); and
- publicly available sources (for example scientific or professional literature).

If your Personal Data is disclosed to us by an individual third party, we will assume that you have authorised that person to use and disclose your Personal Data to us. It is the responsibility of that person to ensure that they have the necessary authorisation before doing so. Likewise, if you disclose to us Personal Data relating to another individual, we will assume that you are authorised by that individual to do so. Where such third party is instructed to provide us your Personal Data, the Personal Data will be processed in accordance with this Privacy Policy.

Where we process your Personal Data obtained from a third-party legal entity, that entity is responsible for providing you with all information required by applicable data protection law, including information about the disclosure of your Personal Data to us. If you have not received this information, please contact that third-party legal entity directly.

4. Purposes and legal titles for processing of personal data

Purpose of processing Personal Data	Scope of Personal Data	Legal title (Art. 6, (1)) of GDPR
Management of public and commercial relations, communication, marketing and business development	Identification data, contact details, professional and role-related data, communication content and signatures, event and marketing communication data, social media data, online identifiers and technical data	F B A
Registration, manufacture, import, export and distribution of medicinal products and medical devices	Identification data, contact details, professional and role-related data, contract and transaction data, product safety, quality and pharmacovigilance data, communication content and signatures	C B F
Management of product quality and pharmacovigilance systems	Identification data, contact details, product safety, quality and pharmacovigilance data, professional and role-related data, communication content and signatures, special categories of Personal Data (Sensitive Personal Data – health data)	C Sensitive Personal Data – Art. 9 (2) h, i

Safeguarding high standards of quality and safety of health care and medicinal products or medical devices	Product safety, quality and pharmacovigilance data, identification data, contact details, professional and role-related data, visitor and site security data (where relevant), special categories of Personal Data (Sensitive Personal Data – health data)	C E Sensitive Personal Data – Art. 9 (2) h, i
Recruitment and human resources management, occupational health and safety and emergency management	Identification data, contact details, recruitment and HR-related data, professional and role-related data, communication content and signatures, visitor and site security data, whistleblowing and compliance data (where relevant), special categories of Personal Data (Sensitive Personal Data – health data, where required by law)	B C F Sensitive Personal Data – Art. 9 (2) b, h, i
Management and performance of commercial and other contracts	Identification data, contact details, professional and role-related data, contract and transaction data, communication content and signatures, event and marketing communication data (where linked to contracts)	B C F
Management of financial and accounting processes, financial resources and legal reporting	Identification data, contact details, contract and transaction data, communication content and signatures, whistleblowing and compliance data (where relevant), document and archiving-related data (embedded categories)	C F
Management of corporate governance and compliance with applicable legal and regulatory requirements	Identification data, contact details, professional and role-related data, contract and transaction data, whistleblowing and compliance data, communication content and signatures, document and archiving-related data, product safety, quality and pharmacovigilance data (where relevant), vehicle, accident and insurance data (where relevant)	C E F Sensitive Personal Data (if involved) – Art. 9 (2) f, g
Provision of legal assistance and representation, handling of claims and disputes	Identification data, contact details, contract and transaction data, communication content and signatures, product safety, quality and pharmacovigilance data, visitor and site security data, vehicle, accident and insurance data, whistleblowing and compliance data, special categories of Personal Data (Sensitive Personal Data – where necessary for legal claims)	C F Sensitive Personal Data (if involved) – Art. 9 (2) f
Management of IT resources and information security	Online identifiers and technical data, identification data (user accounts), contact details (linked to accounts), professional and role-related data, communication content and signatures (e.g. Logs), management of internal registrations and internal records	C F
Document and archiving management	All categories of personal data contained in documents and records processed under other purposes (in particular: identification data, contact details, professional and role-related data, recruitment and HR-related data, contract and transaction data, communication content and signatures, product safety, quality and pharmacovigilance data, vehicle, accident and insurance data, whistleblowing and compliance data)	C F
Physical security and protection of individuals, property and operational activities	Identification data, contact details (where necessary), visitor and site security data (including arrival/ departure time, destination, training records, image without facial recognition), vehicle, accident and insurance data, communication content and signatures, general health	C F Sensitive Personal Data (if

	screening data (e.g. Temperature, symptoms, exposure – as part of site entry requirements)	involved) – Art. 9 (2) b, i
Management of internal registrations and internal records	Identification data, contact details, professional and role-related data, recruitment and HR-related data, contract and transaction data, communication content and signatures, online identifiers and technical data, whistleblowing and compliance data (where relevant)	C F
Protection of Zentiva's assets and the assets of its customers and suppliers	Identification data, contact details, professional and role-related data, visitor and site security data, vehicle, accident and insurance data, contract and transaction data, online identifiers and technical data, communication content and signatures	C F
Event organisation and support	Identification data, contact details, professional and role-related data, event and marketing communication data, communication content and signatures, social media data, image and voice data (photos, videos, audio recordings)	F B A

A – Art. 6(1)(a) GDPR – consent
Processing based on your freely given, specific, informed and unambiguous consent.

B – Art. 6(1)(b) GDPR – contract
Processing necessary for the performance of a contract with you or to take steps at your request before entering into a contract.

C – Art. 6(1)(c) GDPR – legal obligation
Processing necessary for compliance with a legal obligation to which we are subject.

E – Art. 6(1)(e) GDPR – public interest / official authority
Processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

F – Art. 6(1)(f) GDPR – legitimate interests
Processing necessary for the purposes of our legitimate interests or those of a third party, except where outweighed by your interests or fundamental rights and freedoms.

Art. 9(2)(b) GDPR – employment and social protection
Processing of special categories of data necessary for carrying out obligations and exercising specific rights in the field of employment, social security and social protection law.

Art. 9(2)(h) GDPR – health and social care
Processing necessary for the purposes of preventive or occupational medicine, medical diagnosis, provision of health or social care or treatment or the management of health or social care systems and services.

Art. 9(2)(i) GDPR – public interest in the area of public health
Processing necessary for reasons of public interest in the area of public health, such as protection against serious cross-border threats to health and ensuring high standards of quality and safety of health care and medicinal products or medical devices.

Art. 9(2)(f) GDPR – legal claims
Processing necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

Art. 9(2)(g) GDPR – substantial public interest
Processing necessary for reasons of substantial public interest on the basis of law which is proportionate to the aim pursued and provides for suitable safeguards.

5. Retention period

We keep your Personal Data only for as long as necessary for the purposes described in this Privacy Notice. In case you have any questions on retention of your personal data, please contact us on email: dpo@zentiva.com.

6. Processors and Personal Data recipients

Processors

Category of Processor	Processing activity
IT and cloud service providers	Provision, hosting, maintenance and support of our IT systems, applications, communication tools and cloud services, including security, backup and storage of Personal Data
Providers of operational support services	Operational support such as printing, mailing and courier services, call centre services, document scanning, archiving and secure destruction of documents and media
Security service providers	Ensuring physical security of our premises and assets, including access control, reception services and monitoring by external security agencies, in accordance with our instructions
HR and recruitment service providers	Support in recruitment and HR processes, including candidate sourcing, applicant tracking systems, training platforms and administration of certain HR-related processes
Payroll, accounting and administrative service providers	Processing of payroll, benefits and other HR-related payments, as well as administrative and accounting services carried out on our behalf
Occupational health and safety service providers	Provision of occupational health services, health and safety trainings, risk assessments and other workplace safety services required by law or our internal rules
Pharmacovigilance and regulatory support providers	Assistance with collection, assessment, reporting and documentation of adverse events and quality complaints and with other regulatory obligations for medicinal products and medical devices
Marketing, communication and event service providers	Organisation and support of events, preparation and distribution of marketing and communication materials, management of mailing tools, surveys and similar services
CRM, newsletter and customer communication platform providers	Provision and operation of systems used to manage contacts, send newsletters and other communications and record our interactions with customers and business partners.
Receivables management and debt collection service providers	Management, administration and recovery of receivables arising from our contractual relationships, in accordance with our documented instructions and applicable law
External archiving and storage service providers	Secure physical and electronic storage and archiving of Personal Data and related documents and, where applicable, anonymisation or destruction of such data

7. Recipients

Your Personal Data may also be disclosed to third parties who are authorized to obtain such Personal Data. These may include, in particular, the following authorities:

- UK Department for Work and Pensions
- Information Commissioner's Office (ICO)
- National Cyber and Information Security Agency
- Law enforcement authorities (courts, public prosecutors, and the police)
- Occupational health service providers
- Postal service operators
- Companies providing insurance services and claims settlement
- HM Revenue and Customs (HMRC)
- Other applicable public authorities where Zentiva is established

8. Transfers of your Personal Data outside the EU/EEA

We generally process your Personal Data in the Czech Republic and in other EU/EEA countries, where the same data protection rules apply under the GDPR. Only exceptionally we do transfer Personal Data to countries outside the EU/EEA or to international organisations.

If such transfers are necessary (for example within the Zentiva group or to certain service providers), we first assess whether the recipient ensures an adequate level of protection and whether your rights can be effectively enforced in that country. We will transfer your Personal Data outside the EU/EEA only if at least one of the following applies:

The European Commission has adopted an **adequacy decision** for the country or international organisation or we have put in place **appropriate safeguards** in compliance with Standard Contractual Clauses adopted by the European Commission.

Where we transfer your Personal Data from the EU/EEA to recipients in countries without an adequacy decision, we usually rely on the European Commission's Standard Contractual Clauses and, where appropriate, additional technical and organisational measures. You can request more information about these safeguards (including a copy of the Standard Contractual Clauses) by contacting us at:

- ✓ post: **U Kabelovny 529/16, 102 00 Praha 10 – Dolní Měcholupy, Czech Republic**
- ✓ e-mail: **dpo@zentiva.com**

If Personal Data is provided to a Zentiva entity established outside the EU/EEA, processing of that Personal Data is subject to rules applicable for such Zentiva entity. From the moment we receive your Personal Data, we will process it in accordance with this Privacy Notice.

9. Security and accuracy of your Personal Data

Zentiva processes your Personal Data using appropriate technical and organizational measures designed to ensure its security and confidentiality, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. We apply internal policies, procedures and trainings on data protection and regularly review and update these measures. However, because the internet is an open system, the transmission of information over the internet can never be completely secure; any Personal Data you send to us online is therefore at your own risk and you should ensure it is transmitted securely. We also take reasonable steps to ensure that the Personal Data we process is accurate, complete and, where necessary, kept up to date, and that inaccurate or incomplete Personal Data is erased or corrected without undue delay. From time to time, we may ask you to confirm the accuracy of your Personal Data, and you can always contact us to request rectification, completion or erasure of your Personal Data, as described in the section on your data protection rights.

10. Your rights in relation with your Personal Data

Unless otherwise required by law, you have in particular the following rights in relation to the Processing of your Personal Data:

- **Right of access** – to obtain confirmation whether we process your Personal Data and, if so, to receive a copy of your Personal Data and information on how we process it.
- **Right to rectification** – to have inaccurate Personal Data corrected and incomplete Personal Data completed without undue delay.
- **Right to erasure ("right to be forgotten")** – to request the deletion of your Personal Data, for example where it is no longer needed for the purposes for which it was collected, where you have withdrawn your consent (and there is no other legal basis), where you have successfully objected to the processing, or where the Personal Data has been unlawfully processed or must be erased to comply with a legal obligation. This right does not apply where processing is necessary, for example, for freedom of expression and information, to comply with legal obligations or tasks in the public interest, for reasons of public health, for archiving, scientific or historical research or statistical purposes (where erasure would seriously impair these objectives), or for the establishment, exercise or defence of legal claims.

- **Right to restriction of processing** – to request that we restrict the processing of your Personal Data, for example where you contest its accuracy (for a period enabling us to verify it), where processing is unlawful and you prefer restriction to erasure, where we no longer need the data but you require it for legal claims, or where you have objected to processing and we are verifying whether our legitimate grounds override yours.
- **Right to data portability** – where processing is based on your consent or on a contract and carried out by automated means, to receive the Personal Data you have provided to us in a structured, commonly used and machine-readable format and to have it transmitted to another Controller, where technically feasible.
- **Right to object** – to object at any time, on grounds relating to your particular situation, to processing based on our legitimate interests or on the performance of a task carried out in the public interest or in the exercise of official authority (including any profiling based on these grounds). We will no longer process your Personal Data unless we demonstrate compelling legitimate grounds which override your interests, rights and freedoms, or where processing is necessary for the establishment, exercise or defence of legal claims.
- **Right to withdraw consent** – where processing is based on your consent, to withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing based on consent before its withdrawal.
- **Right to file a complaint** – to file a complaint with the competent Data Protection Authority if you consider that the processing of your Personal Data infringes data protection law.
- **Right not to be subject to automated decisions** – to not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you, except where such processing is necessary for entering into or performing a contract with you, is authorised by law (which also provides for appropriate safeguards), or is based on your explicit consent. At present, you are not subject to decisions based solely on automated processing, including profiling, that produce such effects.

11. How to exercise your rights and how to contact us

Except for your right to file a complaint with the Data Protection Authority, you may exercise your rights by sending us a written request:

- by e-mail: **dpo@zentiva.com**
- by post: **Zentiva, U kabelovny 529/16, 102 00 Praha 10 – Dolní Měcholupy, Czech Republic**

Any questions or concerns you may have about this Privacy Notice or on how we Process your Personal Data may be addressed to the Data Protection Officer at:

- e-mail address: **dpo@zentiva.com**
- company's headquarter address: **Zentiva, U kabelovny 529/16, 102 00 Praha 10 – Dolní Měcholupy, Czech Republic**

We will respond without undue delay and, in any event, within one month of receiving your request. If your request is complex or we receive numerous requests, this period may be extended by up to two additional months. In such a case, we will inform you of the extension and the reasons for the delay within one month of receiving your request.

12. Direct marketing

In addition to the way described in all marketing communication to you, you can unsubscribe from list of recipients of marketing communication at any time by contacting the Data Protection Officer as above.

13. Privacy policy for minors

Our Site(s) is (are) directed at an adult audience. We do not purposely process Personal Data of any individual we know to be under 16 years of age. The Personal Data of the individuals under 16 years of age shall be processed only with the prior consent of the parent or holder of parental responsibility. Such legal representative shall be entitled, upon request, to view the information provided by the individuals under 16 years of age and / or to exercise the rights as detailed herein.

14. The revisions of this Privacy Notice

We regularly review the Privacy Notice, with no prior notice. We encourage you to periodically visit the Privacy Notice, in order to be informed about how we process your Personal data.

15. The Glossary

- "**Affiliate**" shall mean any person that at such time is Controlled by or is under common Control of Zentiva Pharma UK Limited, Company No. 02158996, with its seat at 12 New Fetter Lane, EC4A 1JP, London, UK. It being understood that, for the purposes of this document, the term "Control" (and its grammatical variations) shall mean (i) possession, direct or indirect, through one or more intermediaries, of the power to direct the management or policies of a person, whether through ownership of voting securities, by contract relating to voting rights or otherwise, or (ii) ownership, direct or indirect, through one or more intermediaries, of more than fifty percent (50%) – or any other percentage as per any applicable law which enables to exercise the Control – of the outstanding voting securities or other ownership interest of such person.
- "**Controller**" means the entity that decides how and why Personal Data is processed. In many jurisdictions, the Controller has primary responsibility for complying with applicable data protection laws.
- "**Data Protection Authority**" means an independent public authority that is legally tasked with overseeing compliance with applicable data protection laws.
- "**EEA**" means the European Economic Area.
- "**Healthcare Professional**" means person who works in the health care sector, medicine sector or related industries. It can be, e.g. a doctor, an employee of a hospital, a pharmacist.
- "**Personal Data**" means information that is about any individual, or from which any individual is directly or indirectly identifiable, in particular, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.
- "**Process**", "**Processing**" or "**Processed**" means anything that is done with any Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Processor**" means any person or entity that Processes Personal Data on behalf of the Controller (other than employees of the Controller).
- "**Sensitive Personal Data**" means Personal Data about race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sexual life, any actual or alleged criminal offences or penalties, national identification number, or any other information that may be deemed to be sensitive under applicable law.
- "**Site**" means any website operated, or maintained, by the Company / Zentiva or on Company's / Zentiva's behalf.
- "**Standard Contractual Clauses**" means template transfer clauses adopted by the European Commission or adopted by a Data Protection Authority and approved by the European Commission.

16. The Zentiva entities, branches forming joint controllers

The list of Zentiva affiliated entities and branches acting as joint controllers can be found at https://www.zentiva.com/-/media/files/zentivacom/gdpr/Zentiva-Entities.pdf.