PRIVACY POLICY and its Annexes (A and B)

and PRIVACY NOTICE (*ex* art. 13 of EU Regulation 679/2016)

Preamble

pursuant to European Regulation no. 679/2016 (hereinafter **Regulation**) and national legislation on personal data protection (hereinafter collectively **Privacy Legislation**), we invite you to read this document carefully, as it contains important information regarding the protection of your Personal Data (**your Personal Data**).

The processing of your Personal Data by WYDE is based on the principles of lawfulness, fairness, transparency, purpose limitation, storage limitation, data minimisation, accuracy, integrity, and confidentiality, in accordance with the provisions of the Regulation.

The Annexes to this Privacy Policy (Annex A and Annex B) form an integral and substantial part thereof and are hereby expressly incorporated by reference.

1. DATA CONTROLLER

The data controller for your personal data is WYDE S.r.l. SB, with registered office in Milan, viale Piave no. 21, e-mail: privacy@wyde.it (hereinafter **WYDE** and/or **Controller**), represented by its legal representative *pro tempore*.

2. DATA PROCESSORS

Your Personal Data may be processed by companies, consultants and/or professionals engaged as Data Processors to carry out activities related to the processing of Personal Data on behalf of WYDE. The Controller has drawn up a **list of Data Processors**, which is constantly updated and made available to you upon request at the addresses indicated in section 12 of this Notice.

3. PERSONAL DATA PROCESSED

- Personal identification data (such as name, surname, date of birth, age, gender, etc.)
- Contact data (e-mail, address, telephone number)
- Geolocation data (including “IP” addresses)
- browsing data (including data derived from the use of social icons and social login buttons – e.g.

Facebook, *Instagram*, *LinkedIn*, etc. –) collected through *cookies* installed on your computer or mobile device (for further information please consult the ***Cookie Policy***)

- Banking data useful for the management of the commercial relationship
- Photographic images and/or video footage, collected in connection with participation in training courses, *team-building*, promotions, *contests* and events, exhibitions, shows, performances, museum contexts and installations in general.
- Data relating to your interactions with our *website* or *social media channels* including but not limited to: (i) participation in *test*, questionnaires, initiatives, contests, promotions, events (including through our social channels); (ii) registration for participation in our events (including training courses) by you and/or your collaborators and/or employees; (iii) usage data of the tools made available to you for training plans; (iv) interactions with our social media channels (likes, comments, images and in general any content and information you may publish on the Social Network pages dedicated to our WYDE products and services)

4. PURPOSES AND LEGAL BASIS OF PROCESSING

According to the needs related to access to the various sections of the WYDE website (and subject to specific initiatives requiring the provision of specific Personal Data, for which specific notices will be published from time to time), the purposes of processing Personal Data and the corresponding legal bases are set out below:

Website Registration: the registration procedure, through the creation of an account or the use of an existing social network account, aims to allow the use of the WYDE portal as a "Registered User" and to access a range of exclusive services offered through the same applications. The provision of data is optional. The legal basis for processing is the performance of *contractual measures to which the data subject is party*.

Management of requests and/or initiatives: Personal Data will be collected in order to respond to requests sent to us by e-mail, via website/app and/or via social media, including but not limited to those (a) related to courses and activities offered by WYDE, (b) management of participation in our initiatives (such as, by way of example and not limitation, sustainability activities, games, *team-building*). The legal basis for such processing is the legitimate interest of the Controller. The services referred to in point (a) may also be provided via video chat/call. In such case, the video chat/call support will be activated at the user's discretion, will take place exclusively in live mode and no recording of their content will be made.

Marketing: subject to your express consent, we may process your Personal Data in order to send you, by automated or electronic means and, in particular, by e-mail/SMS/App, commercial communications and to invite you to take part in our promotional initiatives. The legal basis for such processing is the *data subject's consent,* which may be withdrawn at any time.

Participation in Masterclasses or Courses: we may process your Personal Data in order to allow your registration for and use of our Masterclasses and training courses. The legal basis for processing is *the performance of the Contract to which the data subject is party*.

Profiling: subject to your express consent, we may process your Personal Data for profiling purposes, i.e. to analyse or predict your tastes, potential habits and consumer choices in order to offer you personalised products, services, promotions and commercial communications, or for analytical purposes. The legal basis for such processing is the *data subject's consent*, which may be withdrawn at any time. Profiling activities may also be carried out through the use of first-party and third-party cookies. We therefore invite you to read our ***Cookie Policy***. Such processing may be carried out subject to you providing a further specific and optional consent.

Purposes of analysis and improvement of products and services: Personal Data relating to your interactions

with WYDE products and services will be processed to analyse and improve the products and services offered, as well as customer satisfaction, to evaluate the effectiveness of activities and initiatives promoted by WYDE, and to conduct statistical analyses. The legal basis for processing is *the legitimate interest of the Controller* for processing.
Any further purpose in relation to which you have expressly provided your consent, which may be withdrawn at any time.

5. NATURE OF DATA PROVISION

The provision of your Personal Data, depending on the purpose pursued, may be optional or mandatory. When the provision is mandatory, it means that failure to communicate the requested personal data may prevent you from using certain services (e.g., to place orders and make purchases it is necessary to provide an address; failure to provide this information prevents completion of the order/purchase). When the provision is optional, you will be able to use the basic services but not the additional ones (for example, failure to give consent to receive promotional communications will not affect the completion of an order/purchase, but will make it impossible to stay updated on our promotions and initiatives).

The mandatory or optional nature of the provision will be indicated on a case-by-case basis through the use of symbols (e.g. "*") placed next to the information whose provision is mandatory to pursue the respective purpose.

6. METHODS OF PROCESSING

Your Personal Data will be processed in compliance with the provisions of current Privacy Legislation, both with the aid of electronic and automated means, including Artificial Intelligence (AI) systems, including generative AI, and through manual methods, with logic strictly related to the purposes of processing, by means of databases, electronic platforms managed by WYDE or by third parties (appointed as Data Processors), the integrated IT systems of WYDE and the aforementioned third parties, and/or websites owned or used by WYDE.

Your Data will be processed in a manner designed to ensure maximum security and confidentiality, and only by persons trained and authorised to process them. The Controller adopts adequate technical and organisational measures to ensure a level of security appropriate to the risk of the processing.

Personal Data are processed primarily at the Controller's registered offices and at the locations of the Data Processors.

7. SHARING AND TRANSFER OF PERSONAL DATA

Your Personal Data may be made accessible, for the purposes described above, to WYDE employees and collaborators.

The personal data you have provided may be transferred to WYDE Group companies and/or third-party companies, both within and outside the European Union/European Economic Area. Such companies carry out the aforementioned activities relating to the processing of personal data on the basis of a data processing agreement signed between the parties. In particular, where your request concerns a different area or another company, collaborator or professional forming part of the WYDE *team* team for contractual purposes, your personal data may be transmitted to such parties so that they may directly handle your request.

Transfers of personal data to external members of the WYDE *team* team (e.g.: consultants, professionals, contract lecturers) and/or third-party companies located outside the EU/EEA are carried out in accordance with

Chapter V of the GDPR, as further specified in **Annex A** below, which also includes reference to the Standard Contractual Clauses (SCC) approved by the European Commission and attached hereto *as* **Annex B**.

Your Data may also be transmitted to judicial authorities where necessary and in the cases provided for by law.

8. DATA RETENTION PERIOD

In order to ensure compliance with the principles of necessity and proportionality of processing, different retention periods for Personal Data have been identified in relation to the individual purposes pursued:

Website/APP Registration: The Personal Data you provided to register on the website/APP will be retained for the entire duration of your registration on the portal. In the event of inactivity for 36 months, your account will be deleted, unless there are active subscriptions.

The *billing data* will be retained for a period of time necessary to ensure the correct performance of the contract and in any case for a further 10 (ten) years for the purposes of fulfilling the related administrative, fiscal and legal protection obligations.

Data collected for the management of ***competitions and prize operations*** will be retained for the entire duration of the prize operation and for a period sufficient to ensure its correct execution. This is without prejudice to the fulfilment of administrative and fiscal obligations, in relation to which the data retention period is that provided for by law.

Personal data processed for **participation in masterclasses or courses** will be processed for the duration of the course and for the time necessary to allow the correct management of participation in the course itself and the related administrative requirements. Any participation certificates will be retained for the duration of the validity of your Account.

Data collected for ***profiling*** and for ***marketing*** purposes, for which you have provided consent to processing, will be retained for a period of 36 months.

Data collected for the purposes of analysis and improvement of products and services will be processed for the period considered strictly necessary to achieve such purposes, after which they will be anonymised.

Data collected for the management of and response to requests in relation to WYDE products and initiatives, and data provided in interactions with the WYDE world, will be retained for the period necessary to process the requests and subsequently anonymised where no further contact takes place, subject to any administrative obligations (for example, a request relating to a complaint must be retained beyond its management period for administrative purposes).

9. MINORS' DATA

WYDE does not normally intend to collect Personal Data of minors or deliberately establish communication with them. For this reason, we invite parents to actively monitor the online activities of children under the age of 16 (sixteen).

Notwithstanding the foregoing, in the event that WYDE needs to contact a minor under 16 (sixteen) years of age, the consent of the parents or those exercising parental authority will be required.

10. RIGHTS OF THE DATA SUBJECT

You may at any time exercise against the Controller the rights provided for under Arts. 15 et seq. of the Regulation, including:

a. the right to obtain confirmation of the existence or otherwise of personal data concerning you, even if not yet recorded, and their communication in an intelligible form;

b. the right to withdraw at any time the consent you have provided in relation to the purposes of processing;

c. the right to obtain access, rectification, erasure, restriction of processing and portability of personal data;

d. the right to object to processing at any time;

e. the right to lodge a complaint with the competent supervisory authority, where you consider that the processing of your data is contrary to applicable law.

11. HOW TO EXERCISE YOUR RIGHTS

Should you wish to exercise the aforementioned rights, or should you wish to receive further clarification regarding the processing of your personal data, you may write to: WYDE S.r.l. SB, with registered office in Milan, viale Piave no. 21, or by e-mail: privacy@wyde.it.

Notice on the transfer of personal data to Countries outside the EEA (European Economic Area)

Annex A to the WYDE Privacy Policy

Transfers of personal data to countries outside the European Economic Area (**EEA**) may be carried out by WYDE for the purposes of international trade or cooperation. WYDE, in the course of its activities, may need to transfer personal data to a country outside the EEA area, for example when there is a need to share personal data with its business partners or with its suppliers based outside the EEA area.

The GDPR contains specific provisions for such transfers. With these provisions, the GDPR aims to ensure a level of protection for transferred personal data equivalent to that enjoyed within the EEA area.

1. When does a transfer of personal data outside the EEA area occur?

The GDPR does not provide a definition of such transfers. However, the **EDPB** (*European Data Protection Board*) has identified the following three cumulative criteria to identify a transfer outside the EEA area:

- a controller or a processor must apply the GDPR for the processing in question;
- this controller or processor discloses, by transmission, or makes available the personal data of another organisation (controller or processor);
- this other organisation is located in a country outside the EEA area or is an international organisation.

2. How to transfer personal data outside the EEA area?

The GDPR imposes restrictions on the transfer of personal data outside the EEA area, to non-EEA countries or international organisations, to ensure that the level of protection of natural persons afforded by the GDPR remains the same.

Personal data may be transferred outside the EEA area only in compliance with the conditions set out for such transfers in Chapter V of the GDPR. The conditions for transfers must be complied with in addition to compliance with the other provisions of the GDPR in general. For example, these conditions constitute an additional requirement over and above the **fundamental principles of processing**, which must also be complied with in the context of international transfers.

When WYDE transfers personal data, it ensures that it has an adequate legal basis for the processing; that the necessary security measures are in place; that it only processes the personal data necessary for this particular processing activity (data minimisation principle), etc.

If the recipient of the personal data acts as a data processor, they are still legally required to enter into a **contract**. Just as is done for a processor within the EEA area.

Under the GDPR, there are, in principle, two main ways to transfer personal data to a non-EEA country or an international organisation. Transfers may take place on the basis of an adequacy decision or, in the absence of such a decision, on the basis of appropriate safeguards for natural persons, including enforceable rights and effective remedies. In the absence of an adequacy decision or appropriate safeguards, the GDPR allows for certain derogations in specific situations.

Data transfers on the basis of an adequacy decision

The European Commission has the power to adopt adequacy decisions to formally confirm, with binding effect for the EEA countries, that the level of data protection in a non-EEA country or in an international organisation is substantially equivalent to the level of protection in the European Economic Area.

When assessing the adequacy of the level of protection, the European Commission considers as essential such principles as the rule of law, respect for human rights and fundamental freedoms, as well as the effectiveness and enforceability of data subjects' rights, the existence and effective functioning of an independent data protection authority in the non-EEA country and the international commitments entered into by the country or international organisation. If the European Commission decides that the country offers an adequate level of protection and an adequacy decision is adopted, personal data may be transferred to another company or organisation in that non-EEA country without the data exporter, i.e. the entity transferring the data, being required to provide further safeguards or being subject to additional conditions relating to international transfers. In other words, transfers to an "adequate" non-EEA country will be comparable to a transfer of data within the EEA. However, your organisation will still need to comply with the other fundamental principles of the GDPR, as explained above. Adequacy decisions may cover a country as a whole or be limited to a part of it (i.e. a region). Adequacy decisions may cover all data transfers to a country or be limited to certain types of transfers (e.g. of a sector). To date (updated to February 2026) the European Commission has adopted adequacy decisions for:

- *Andorra*
- *Argentina*
- *Brazil*
- *Canada (commercial organisations)*
- *Faroe Islands*
- *Guernsey*
- *Israel*
- *Isle of Man*
- *Japan*
- *Jersey*
- *New Zealand*
- *Republic of Korea*
- *Switzerland*
- *the United Kingdom under the GDPR and the LED, as amended in December 2025 through one renewal decision under the GDPR and one renewal decision under the LED*
- *the United States (commercial organisations participating in the EU-US Data Privacy Framework)*
- *Uruguay*
- *and the European Patent Organisation as providing adequate protection.*

The European Commission updates and publishes the list of its adequacy decisions on the website: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

WYDE, where it acts as a data exporter, is responsible for checking whether the adequacy decisions relevant to its transfers are still in force and are not in the process of being revoked or annulled.

Adequacy decisions do not prevent individuals from lodging a complaint. Nor do they prevent data protection authorities from exercising their powers under the GDPR.

Data transfers on the basis of appropriate safeguards

In the absence of an adequacy decision, WYDE may transfer personal data where appropriate safeguards are provided for the organisation receiving the personal data. In addition, individuals must be able to exercise their rights and have effective remedies available to them.

Art. 46 of the GDPR lists a number of transfer tools containing "appropriate safeguards" that, in the absence of adequacy decisions, may be used to transfer personal data to non-EEA countries. The main transfer tools in Art. 46 of the GDPR, relevant to private organisations, are:

- Standard data protection clauses (SCC);
- Binding corporate rules (BCR);
- Codes of conduct;
- Certification mechanisms;
- Ad hoc contractual clauses.

Standard Contractual Clauses (SCC)

Standard contractual clauses (**SCC**) are a set of standardised contracts that allow WYDE to transfer personal data outside the EEA by providing appropriate safeguards. It is a tool commonly used by many organisations. Pursuant to Article 46(2)(c) of the GDPR, the European Commission has the power to adopt SCCs as an appropriate safeguard for transfers of personal data to non-EEA countries. On 4 June 2021, the European Commission adopted an implementing decision on SCCs for the transfer of personal data to non-EEA countries under the GDPR. WYDE uses, in such cases, the standard contractual clauses provided by the European Commission on its website (https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en – **Ann. B**).

The SCCs address various transfer scenarios and the complexity of modern processing chains. Controllers and processors may use various options, depending on the specific circumstances of the transfer, including:

- controller to controller (C2C);
- controller to processor (C2P);
- processor to processor (P2P);
- processor to controller (P2C), with the processor in the EU and the controller in a third country.

Other important aspects of the SCCs include:

- the possibility of acceding to the clauses for more than two parties;
- the possibility, with some exceptions, of using the SCCs when transferring personal data to a sub-processor in a non-EEA country;
- the possibility, with some exceptions, for natural persons to invoke the clauses as third-party beneficiaries;
- rules on liability between the parties in the event of a breach of the rights of individuals;
- the right of individuals to compensation for damages suffered in the event of a breach of their rights as third-party beneficiaries;
- the obligation to carry out a "transfer impact assessment" documenting the specific circumstances of the transfer, the laws of the destination country and the supplementary safeguards put in place to protect personal data;
- the obligations in the event of access by public authorities to the transferred data, such as the obligation to provide information to data exporters and to challenge unlawful requests.

WYDE adopts the SCCs referred to in Annex B to its Privacy Policy.

Binding Corporate Rules (BCR)

Binding corporate rules (BCR) that contribute to ensuring an adequate level of protection for data exchanged within a group of companies located both inside and outside the EEA area, are more suited for a multinational group of companies carrying out a large number of data transfers. WYDE is a Benefit Company, a small-sized Innovative SME, and processes data strictly limited to the proper performance of its services.

Codes of Conduct

WYDE also follows the EDPB guidelines and codes of conduct available on the relevant website and constantly updated:

https://www.edpb.europa.eu/system/files/2022-10/edpb_guidelines_codes_conduct_transfers_after_public_consultation_it.pdf)

Final Considerations

In the judgment **C-311/18 (Schrems II)** of 2020, the Court of Justice of the European Union (CJEU) highlighted the possible need for organisations to provide supplementary measures in addition to appropriate safeguards, when transferring personal data outside the EEA area.

Standard Contractual Clauses (SCCs) and other transfer tools referred to in Article 46 of the GDPR do not operate in isolation. The CJEU held that controllers or processors acting as exporters are responsible for verifying on a case-by-case basis whether the law or practice of the non-EEA country affects, for example due to legislation requiring access to data, the effectiveness of the appropriate safeguards relating to the transfer tools contained in Article 46 of the GDPR.

To assist exporters in the complex task of assessing the countries receiving the data and identifying, where necessary, appropriate supplementary measures, the EDPB has adopted recommendations.

Data transfers on the basis of derogations

In addition to adequacy decisions and the transfer tools of Article 46 of the GDPR, the GDPR contains a third avenue that allows for the transfer of personal data in certain situations. Subject to specific conditions, you may still be able to transfer personal data on the basis of a derogation under Article 49 of the GDPR.

Art. 49 of the GDPR is of an exceptional nature. The derogations must be interpreted in a way that does not contradict the very nature of their extraordinary character as exceptions to the rule that personal data cannot be transferred to a country not belonging to the EEA area, unless that country provides an adequate level of data protection or, alternatively, appropriate safeguard measures. The derogations cannot become, in practice, "the rule", but must be limited to specific situations.

Under Article 49 of the GDPR, a transfer, or a set of transfers, may be carried out when the transfer is:

- made with the explicit consent of the individual;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual measures taken at the request of the data subject;
- necessary for the performance of a contract concluded in the interest of the individual between the controller

and another person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defence of legal claims;
- necessary to protect the vital interests of the individual in question or of other persons, where the individual is physically or legally incapable of giving their consent; or
- made from a register which under the national law of an EEA country or Union law is intended to provide information to the public (and which is open to the public in general or to those who can demonstrate a legitimate interest in inspecting such register).

To assess the necessity of the transfer, a "necessity test" must be applied. This test requires assessing whether a transfer of personal data can be considered necessary for the specific purposes of the derogation in question.

When none of the above derogations is applicable to a specific situation, it is possible to transfer the data for compelling legitimate interests of the controller.

However, such transfers are only permitted if the transfer:

- is not repetitive (similar transfers are not carried out on a regular basis);
- involves only data relating to a limited number of individuals;
- is necessary for compelling legitimate interests pursued by the organisation (provided that the interests of the individual do not override such interests);
- is subject to appropriate safeguards put in place by the organisation (in light of an assessment of all the circumstances relating to the transfer) to protect the personal data;
- is not carried out by a public authority in the exercise of its public powers.

In such cases, organisations are required to inform the competent data protection authority of the transfer and to provide further information to natural persons.

In general, derogations should be used only as a last resort for framing a data transfer: organisations should, first and foremost, assess whether it is not possible to rely on an **adequacy decision** or on an **appropriate safeguard**.

When relying on the derogations of Article 49 of the GDPR, it should be noted that organisations transferring data must also comply with other provisions of the GDPR (such as having a legal basis for the communication of data, implementing security and data minimisation measures, signing a contract if the recipient is a data processor, etc.).

Annex B

SCC Clauses

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914