

## Privacy Policy

This is the "regulation on the Protection of privacy, " (hereinafter the "rules") of OneTec SRL, (hereinafter "OneTec" or the "employer").

### 1. **Who are we?**

Organizing an event is always an important challenge for agencies. They spend all their energy in thousands of details in order to have happy visitors and organizers.

OneTec's goal is to improve organizers' efficiency and to create a unique customer experience by using cutting edge innovation.

OneTec's story starts as a Software Developers' Company in early 2000. The first major event OneTec worked for was in 2002 on a huge international medical congress and since, OneTec never stopped working in this sector.

The expansion of Onetec occurred by organic growth, but also with some major acquisitions: Cerix (Belgian leading company in short term IT rental), AIM (company specialized in Voting Systems), Whos-in (ticketing and access control company), Getyoo (specialized in interactive services for visitors on public and professional fairs), Bebotics (specialized in photobooths and custom event experiences) and Eventattitude (leader in Brand Activation interactive & personalised experiences).

Today, OneTec's services consist of 3 main axes: Event Technology, Brand Activation and IT/AV rental.

We take your privacy seriously and are committed to comply with data protection laws, and especially the General Data Protection Regulation (GDPR).

OneTec is a company existing and operating under Belgian law, with statutory seat located at Leuvensesteenweg 542/C4, 1930 Zaventem and registered at the Crossroads Bank for Enterprises under company number 0478.88.94.93.

We use our best efforts to bring the data processing activities of OneTec into compliance with applicable data protection legislation, including Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and the Belgian Data Protection Act of 8 December 1992, each as applicable, and as amended, restated or replaced from time to time.

### 2. **Which data?**

- Are considered as confidential information within the meaning of this Regulation:  
All the employer information that have not been made public. Confidential information that have been made public illegally must also be considered as confidential information;
- All the personal data, as defined by the GDPR, namely:  
« Any information relating to an identified or identifiable natural person; is deemed to be an "identifiable individual", meaning a natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, online id, or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity ».

Hereinafter referred to as the "confidential information".

We most commonly but not always, process the following categories of confidential information about you:

- Your personal data (last name, first name, address, city, country);
- Your professional data (company, job title);
- Your email address;
- The picture representing you and the other persons on the picture;
- On an aggregated basis, limited socio-demographic data: your gender (female-male-undefined), your age (or range), your language;
- The answers that were asked by our client and that you were invited to fill in.

We process your confidential information for the following purposes, only with your consent:

- Sending your registration confirmation, reminder, thank you message or post-event survey;
- Sending documents related to the event;
- Sending your picture to your email address;
- Posting your picture on a privately accessible photo gallery;
- Transfer your picture to our client as well as your given information to the questions our client asked so that they can know you better. Our client is not authorized to use your personal data for marketing purposes and will not use your picture for corporate internal or external communications (e.g. post your picture on its own social media accounts or website) unless consent was asked and given by you;
- Transfer your picture and your email address to our client so you can receive special offers and promotions from our client;
- Transfer your picture to our client so that it may be used for corporate internal or external communications (e.g. post your picture on its own social media accounts or website);
- Transfer your picture and your email address to our client and provide our client with socio-demographic insights for our client to tailor its marketing activities.

### **3. Employees' commitment**

This regulation contains directives to be respected by all OneTec's employees in the exercise of their functions. Employees come into contact with confidential information in the performance of their duties. Employees must maintain the confidential information at any time under the seal of secrecy and won't share them with anyone else then authorized colleagues, after checking, to access the confidential information in question.

The employees are committed not to share confidential information voluntarily or involuntarily with unauthorized persons, including third parties.

The employees are also committed to never use the confidential information at the expense of the employer, or for any other purpose than those of their mission.

These commitments are the subject of an internal contract agreed by all the employees, including members of the Board of Directors, the management, volunteers, interns, sub-processors, clients, etc. (hereinafter the "collaborators") and, therefore, any person who comes into contact with confidential employer information or information that may be considered as personal data under the GDPR-regulation.

### **4. Your rights**

Subject to applicable data protection laws, you have the rights to access, rectify and erase your personal data, the rights to object to or limit the processing of your personal data and the right to data portability, meaning that:

- You have the right to be informed about how we use your personal data and how to exercise your rights.
- You have the right to be provided with clear, transparent and easily understandable information about how we use your personal data and your rights;
- ➔ Therefore, this is all mentioned on every screen we use asking / collecting your personal information and you have the right not to complete this.
- You have the right to obtain access to your personal data. This is so you are aware and can check that we are using your personal data in accordance with applicable data protection laws;
- You have the right to request the deletion of your personal data where there is no compelling reason for us to keep using it. Please note that this is not an absolute right to erasure and exceptions apply.
- You are entitled to have your personal data rectified if they are inaccurate or incomplete;
- You have 'the right to be forgotten' and, in simple terms, this enables you to request the deletion or removal of your personal data where there is no compelling reason for us to keep using it. This is not an absolute right to erasure and exceptions apply;
- You have rights to 'block' or suppress further use of your personal data. When processing is restricted, we can still store your personal data, but may not use it further;
- You have rights to obtain and reuse your personal data for your own purposes across different services;
- You have the right to lodge a complaint about the way we handle or process your personal data with your national data protection authority;
- If you have given your consent to anything we do with your personal data, you have the right to withdraw your consent at any time (although if you do so, it does not mean that anything we have done with your personal data with your consent up to that point is unlawful).

Please forward any request regarding your rights as data subject to us by email at [info@onetec.eu](mailto:info@onetec.eu). We will try to comply with your request as soon as reasonably practicable and always under the timeframes set forth by applicable data protection law. Please note that we may need to retain certain of your personal data for certain purposes as required or authorized by law. We may also ask you for a proof of identity if we have a doubt about your it.

#### **5. Protection of confidential information / Security measures**

Legally if we received your personal data with your consent and with a legitimate interest to collect and disclose them to our client, we are in our rights.

We will ask for your free, prior and informed consent if our clients want to use your personal data for direct marketing purposes or want to publish your picture online (on their social media accounts or in their websites) or use it for internal or external corporate communications. By giving your consent to our client, you irrevocably waive any claim for (economic) compensation for the use by our client of your picture or personal data.

The provision of your personal data is necessary for the legitimate interests pursued by OneTec provided that these interests prevail over your fundamental rights and freedoms.

We do not subject you to decisions based exclusively on automated processing that produces legal effects concerning your or similarly significantly affect you.

The provision of your picture and your personal data (i.e. email address) is a necessary condition for the provision of our service. If we cannot process your picture or your email address, you may not use our service.

We do not collect personal data about you from third parties.

We have analysed the risks and reassess them specifically for each data collected (implementation of measures adapted to the risk). Treatment in the legitimate interests of the customer / organized by a contract which regulates the use of the data and the protection.

The data collect is done according to the rules of the GDPR: always with application for free, revealed specific consent by an event active.

In addition to that: you can read all security measures taken by us, mentioned in this Privacy Policy.

## **6. Transport of confidential information**

**In case of transport of confidential information (e.g. on an USB key or a laptop outside of the business premises), the employees take into account the following guidelines:**

- Employees limit the transport of confidential information within and exclusively to what is strictly necessary for the performance of their work;
- The employees need to be aware permanently of the risk of data loss in this type of situation;
- The employees must do everything that is in their power to prevent the theft or loss of data (e.g. forgetting their computer laptop/smartphone on the train, theft of their laptop left in the car...);
- Employees must never leave their laptop unattended outside of the work place;
- The employee's victims of a theft of their laptop, smartphone or tablet inform their hierarchical superior without delay and at the latest within six (6) hours of discovery of the theft. Employees who find that their laptop, smartphone or tablet has been hacked must inform their hierarchical superior without delay, and no later than six (6) hours of the finding;
- Employees who use another wireless network than that of the employer, must verify if this is a secure network. It is also forbidden for employees to use an open and unsecured WIFI network.

These commitments are the subject of a contract agreed by all the employees, including members of the Board of Directors, the management, volunteers, interns, sub-processors, clients, etc. (hereinafter the "collaborators") and, therefore, any person who comes into contact with confidential employer information or information that may be considered as personal data under the GDPR-regulation.

## **7. Where is my confidential information stored?**

All data are stored in a SQL database, secured by an encrypted login and password. The data center is located in Europe and duplicated in Belgium for security reasons.

The data will be provided to our client, if allowed by GDPR, through an encrypted file.

The data at rest will be deleted by OneTec at the end of the mission.

- Outside OneTec: the servers are physically located by Net7 – our GDPR compliant subcontractor located in Belgium and OVH.

- Inside OneTec: the data only carry through the officers in charge of the project. Each computer is protected by a personal password. The OneTec's building is protected by an alarm system.

#### **8. How long do we retain your personal data?**

We retain your personal data as long as necessary to achieve the purposes for which we process your personal data. OneTec and our clients and sub-processors do not keep data longer than what is necessary in order to carry out the mission for which they were collected and won't pass them on to any third party without explicit authorisation by the participating customers.

We use the following criteria to determine the retention periods of personal data according to the context and purposes of each processing operation:

- The time elapsed since the event;
- The sensitivity of personal data;
- Security reasons (for example, the security of our information security systems);
- Any current or potential dispute or litigation;
- Any legal or regulatory obligation to retain or delete personal data.

When you are invited to give your consent, you are always informed about the retention period to be able to agree to the use of your data knowingly.

#### **9. How can I stop receiving marketing e-mails?**

If you would like to stop receiving e-mails from our clients, you can opt-out at any time by unsubscribing from the mailing list of our client or by sending them an email explaining you do not want to receive their newsletter anymore.

Our clients must provide you with the possibility to object from receiving any type of e-mails e.g. through a link to unsubscribe from their mailing list or by allowing you to send an email to them.

You have the right to object at any time to the processing of your personal data for direct marketing purposes.

You always have the right to lodge a complaint at the competent data protection authority. The competent data protection authority for Belgium can be contacted at:

**Belgian Data Protection Authority / Autorité de protection des données /  
Gegevensbeschermingsautoriteit**  
Rue de la Presse, 35, 1000 Bruxelles / Drukpersstraat 35, 1000 Brussel  
[commission@privacycommission.be](mailto:commission@privacycommission.be)  
+32 (0)2 274 48 00

#### **10. I have a question or a problem. Who can I contact?**

If you have any question or complaint about the processing of your personal data, please contact us by email at [info@onetec.eu](mailto:info@onetec.eu) or by post at Leuvensesteenweg 542/C4, 1930 Zaventem (Belgium).