

Applicable from 13 May 2024



# **BidWork Tender Management Privacy Policy**

## **1. Who we are and scope of this notice**

OFA Group SAS is a subsidiary of Fortius Bidco Group Ltd and part of the Once For All group of companies, and each of their entities referred to below, collectively as ‘the Company’ “we” or “us”, want you to be familiar with how we collect, use and disclose personal data.

OFA Group SAS (registered on the 3<sup>rd</sup> of November 2021 with registration number 904 892 833 RCS Paris and registered office at [53 RUE DE CHATEAUDUN 75009 PARIS](#)) is the provider of the Platform Onceforall (‘the Platform’) and associated services (SaaS) in the European Economic Area and Switzerland. Collectively, we refer to any services provided through the Platform or otherwise available to simple Internet browsers on our websites as “the Services”.

Fortius Bidco Group Limited is a company incorporated and registered in England and Wales with company number 11409619 and with registered office at Midpoint, Alencon Link, Basingstoke, Hampshire, RG21 7PP also known as Constructionline or Facilitiesline which are trading names.

This privacy notice (“Notice” also referred to as “Privacy Policy”) explains how we process personal data while offering the Services to the ‘Buyer’ and/or ‘Supplier’ (referred to as ‘the client’/‘the Customer’) and in our interactions with their authorised personnel (‘the Users’, ‘you’), while using our current and any future websites (for example <https://www2.attestationlegale.fr>; <https://onceforall.com>; <https://onceforall.fr>; <https://www.constructionline.co.uk>) and our platform Onceforall, accessible via portal.onceforall.com and any future platform we might develop.

All references in this Notice to “our website” means the website provided and operated by us also referred to as ‘the Platform’ and, together with the Terms and Conditions, the Terms of Use and our Cookie Policy, this Notice set out the basis upon which you may use the Platform.

Please read this Notice and any other privacy notice or fair processing notice we may provide on specific occasions carefully, as it is designed to help you understand what information we collect from and about you, why we collect it, and why and how we may use it.

## **2. Our commitment**

We respect your right to privacy and are committed to protecting it and complying with the applicable data protection law including the EU GDPR and the UK GDPR. We take our data protection and privacy responsibilities seriously.

We will always keep your personal data safe. We will be clear and open with you about why we collect your personal data and how we use it. Where you have choices or rights, we will explain them to you and respect your wishes in line with legal requirements.

The company carries out personal data processing when it processes the data of its employees, customers, and service providers, and therefore, in this case, is responsible for the processing of data provided directly by the data subjects or collected via the Website as described in this Notice. This means that, in these circumstances, the company determines why this data is collected, how it is collected, how this data will be used and how it will be protected.

As part of the provision of services delivered throughout the Platform, we are data processor with regard to the processing activities that we carry out as part of the service we provide, when Buyers and Suppliers and more generally Customers are acting as Controller for the processing of data generally documents they submit on the Platform.

## **3. Our contact details**

If you wish to contact us directly, please do so at:

**For France:** [rgpd@onceforall.com](mailto:rgpd@onceforall.com) - +33 4 72 38 32 58

**For Germany:** [kontakt.de@onceforall.com](mailto:kontakt.de@onceforall.com) - +49 30 20314 199

**For Belgium:** [support.belgium@onceforall.com](mailto:support.belgium@onceforall.com) - +32 78 48 37 52

**For Italy:** [contatto.it@onceforall.com](mailto:contatto.it@onceforall.com) - +39 02 3056 9038

**For UK:** E-mail: [gdpr@onceforall.com](mailto:gdpr@onceforall.com)

#### **4. Data protection officer (DPO)**

We have appointed GRCI Law Limited as our DPO, who are responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, our privacy practices or how we handle your personal data, please contact our DPO at [dpo@onceforall.com](mailto:dpo@onceforall.com).

#### **5. What is meant by personal data?**

Personal data, sometimes also referred to as personal information, is information which identifies you as an individual or relates to an identifiable individual. Examples of personal data include: your name, address, bank account details, internet protocol (IP) address, username or another identifier.

#### **6. How we collect personal data**

In order to administer, manage and provide our [products and] Services and / to manage our relationship with you, we may collect and use personal data about you. The personal data we collect about you will depend on your relationship with us and can come from different sources including:

#### **Information you give to us directly when you:**

- register for the Platform or otherwise to receive information using our contact us pages;
- fill in forms or surveys;
- engage with the Platform;
- correspond with us by phone, email, chat or otherwise;
- make an enquiry regarding our Services;
- purchase products and / or Services from us.

#### **Information we receive from third parties such as:**

- Device and technical data, for example from the following parties:
  - analytics providers such as Google and Crazy Egg and Hotjar
  - advertising networks;
  - search information providers;
  - providers collecting survey information, such as SurveyMonkey
  - reviews from providers such as Trustpilot;
  - data feeds from third party sites such as Companies House /Public Register
- Contact, financial and transaction data from providers of technical, payment and delivery services, such as Stripe and Pay360.
- Information provided by public authorities/ entities the Customer has authorised us to contact (for example URSAFF in France)

We need to collect certain personal data in order to provide the Services to you. If you do not provide information requested, we may not be able to provide the Services to you either in whole or part.

## 7. The type of personal data we collect

Depending on your relationship with us, we may collect and process the following categories of personal data:

<b>Identity Data</b>	such as your contact name (including first, middle and surname), date of birth and title
<b>Contact Data</b>	such as address / telephone number(s)/ Email address / mobile number
<b>Customer Data ( on the Organisation)</b>	<ul style="list-style-type: none"> <li>• Company name</li> <li>• Legal representative name</li> <li>• Company registration number(s) (SIREN/SIRET for France)</li> <li>• Office locations</li> <li>• Type of work the organisation offers</li> <li>• Geographic area where the organisation operates</li> <li>• Identifiers &amp; passwords for the relevant platforms only if the collection service is enabled</li> </ul>
<b>Customer Data (Organisation workers)</b>	<p>EU employees</p> <ul style="list-style-type: none"> <li>- First and last name</li> <li>- Identity documents</li> <li>- RSI / Financial information / Social declaration</li> </ul> <p>Foreign employees (Outside the EU / Schengen area) containing:</p> <ul style="list-style-type: none"> <li>- First and last name</li> <li>- Country of nationality</li> <li>- Hiring Date</li> <li>- Type and number of residence permit</li> </ul>
<b>Employment Data</b>	such as name, job title, hire dates, company address, business email address and telephone number, and details of your directors and executive officers
<b>Insurance Data</b>	such as insurance company name, address, contact details, policy details, and coverage values
<b>Experience and Qualification Data</b>	such as details of qualifications and certificates including but not limited to work permit / professional cards and equivalents
<b>Location Data</b>	such as your IP address and telephone codes
<b>Transaction Data</b>	such as details about payments to and from you and other details of the Services you have access to on our website or you have purchased from us
<b>Technical Data</b>	including your IP address, your login data, browser type and version, time zone setting and location, browser plugin types and versions, operating system and platform, and other technology on the devices you use to access the Platform
<b>Profile Data</b>	such as your log-in credentials to the Platform, email and password, the Service you have engaged with including the services you have used on the Platform, feedback Survey responses and such information about your health as you voluntarily provide to us

<b>Usage Data</b>	including information about how you use the Platform and the Services you use
<b>Marketing and Communications Data</b>	such as your preferences in receiving marketing material from us and your communication preferences
<b>Recordings</b>	including voice recordings from phone call interactions
<b>Payment Information</b>	such as bank and / or payment card information
<b>Special Category Personal Data [sensitive personal data]</b>	We do not collect sensitive data unless the Customer is instructing us to do so

We may also collect, use and share aggregated data such as statistical or demographic data for any purpose. Aggregated data could be derived from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data with that of others in order to calculate the percentage of users accessing a specific feature of [the Platform]. However, if we combine or connect aggregated data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data, which will be used in accordance with this Notice.

#### **8. Sensitive personal information**

We do not usually collect sensitive personal data including special categories of data unless we are instructed by the Customer to do so. Special category data is personal data that needs more protection because it is sensitive – given the sensitivity of that data, we provide additional specific protection to that information when we process it.

We may collect this type of personal data from you in the course of providing you with our services or during our interactions with you, for example, where you voluntarily disclose to us or upload sensitive data in the platform.

When you are calling us, we may proceed to voice calls recording based on our business legitimate interests. You are systematically informed prior to the recording to start, and you are given the possibility to object.

#### **9. Our legal bases for processing personal data**

We only collect and process your personal information when and how the law allows us to do so; that is, when we are satisfied that we have a lawful basis for doing so.

Most commonly we will use your personal information in the following circumstances:

- Where you have consented before the processing takes place to your employer (our Customer).
- Where we need to perform a contract we are about to enter into, or have entered into with the Customer.
- Where we need to comply with a legal or regulatory obligation or support our Customer to abide its own legal obligations.
- Where the processing is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. When we rely on this legal basis, we will consider and balance any potential impact on you (both positive and negative), and your rights under data protection laws. Where we process personal data for our

own legitimate business interest, we do so in order to manage our business to enable us to deliver the best possible Services to you.

When we process on the lawful basis of legitimate interest, we apply the following tests to determine whether it is appropriate:

- The purpose test – is there a legitimate interest behind the processing?
- Necessity test – is the processing necessary for that purpose?
- Balancing test – is the legitimate interest overridden, or not, by the individual’s interests, rights or freedoms?

The Company has assessed its legitimate interests and found that its data processing activities are in line with clients’ expectations and there are no individual interests that override OFA interests in processing your data as described above. Therefore, OFA concluded that it may process your data for legitimate purposes as long as it does not affect your rights and freedoms in accordance with the regulations in force.

In the table below, you will find the legal bases that we rely on to process your personal data:

<b>PERSONAL DATA PROCESSING PURPOSE</b>	<b>LEGAL BASIS FOR PROCESSING</b>	<b>CATEGORIES OF PERSONAL DATA</b>
<p><b>Contract Administration</b> For example, to enable us to meet our obligations owed to you arising from any agreement proposed or entered into between you and us; to process orders, take, or receive payment, for such orders and / or the provision of Services and deal with refund requests.</p>	<p>Contract Legal Obligation Legitimate interest</p>	<p>Contact Data Identity Data Customer data (on the organisation) Customer data (on the workers) Employment data Experience and qualification data Special category of data Payment data</p>
<p><b>Providing (and Maintaining the Integrity of) our Services</b> For example to run our business, provision of administration and IT services, network security, to prevent fraud, and in the context of a business reorganisation or group restructuring exercise.</p>	<p>Legitimate Interest</p>	<p>Usage Data Profile Data Recording Customer data (on the organisation) Employment Data Technical data</p>
<p><b>Relationship Management</b> For example to manage our relationship with you, which may include, notifying you of changes to our terms or to this</p>	<p>Contract Legal Obligation Legitimate Interest</p>	<p>Contact Data Identity Data Customer Data ( on the organisation)</p>

<p>Notice, contacting you with regard to updates or informative communications related to our Services and managing contact, including to respond to queries and manage complaints.</p>		
<p><b>Conduct Surveys and Gather Feedback</b></p> <p>For example to contact you to ask you to leave a review, provide us with feedback on our products and/or services or take a survey and conducting relevant customer satisfaction follow-up activities.</p>	<p>Legitimate Interest</p> <p>Consent</p>	<p>Marketing and Communication data / Location Data</p>
<p><b>Service Improvement</b></p> <p>For example, assessing the quality of our Services (and service delivery) including to inform the making of changes and improvements to our Services and service delivery, to grow our business and to inform our marketing strategy.</p>	<p>Legitimate Interest</p> <p>Legal Obligation</p>	<p>Usage data</p>
<p><b>Record keeping</b></p> <p>For example in relation to our [products and services] [Services] / usage.</p>	<p>Contract</p> <p>Legal Obligation</p> <p>Legitimate Interest</p>	<p>Usage Data</p>
<p><b>Running Marketing Activities</b></p> <p>For example, managing and running relevant marketing campaigns, including communicating with you to make recommendations to you about services that may interest you; to provide you with marketing content where permitted by law and to ensure that our marketing material is tailored to your interests; to make suggestions and recommendations to you. about goods or services that may be of interest to you.</p>	<p>Consent</p> <p>Legitimate Interest</p>	<p>Marketing and communication data</p>
<p><b>Legal Administration</b></p>	<p>Legal Obligation</p>	<p>All categories of Data</p>

<p>For example, to co-operate with a police investigation and/or comply with a court order as required by law; to enforce or apply our website / Platform terms of use, our policy terms and conditions, and / or other contracts; and/or to exercise our rights, to defend ourselves from claims and to keep to laws and regulations that apply to us and the third parties we work with.</p>		
<p><b>Analysis of Marketing Activities</b></p> <p>For example, measuring and / or understanding the effectiveness of the advertising we serve to you.</p>	<p>Legitimate Interest</p>	<p>Usage data Marketing data</p>
<p><b>Data Analysis</b></p> <p>For example to maintain the currency of, and improve, our website, the Platform and our Services, as well as the marketing of same; to study how customers use our Services in order to develop them, to grow our business and to inform our marketing strategy and to define types of customers for our products and Services.</p>	<p>Legitimate Interest</p>	<p>Technical data Usage data Marketing data</p>

If you would like to find out more about the legal basis for which we process personal data, please contact us. Our contact details are specified above at paragraph 3.

#### **10. Using your data for other reasons**

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose and/or described within our terms and conditions.

#### **11. Withdrawing consent**

If we rely on your consent to process your personal information, which may be express or implied consent according to the applicable law, you have the right to withdraw consent at any time. If you have given consent directly to us, you can withdraw your consent following the withdrawal procedure



presented to you when you gave consent or by contacting us by using the contact details specified under point 3 of this Notice. Please note that this will not affect the lawfulness of the processing which has taken place before you withdrew your consent nor, when applicable law allows, will it affect the processing of your personal information on the basis of any other lawful basis other than consent.

When you have provided the consent to your employer (our Customer) you need to contact your employer directly to be able to action the consent withdrawal procedure.

## **12. Using personal data for marketing purposes**

We may use your personal data to let you know about our Services that we believe will be of interest to you. We may contact you by email. In all cases, we will respect your preferences for how you would like us to manage our marketing activity with you.

To protect privacy rights and to ensure you have control over how we manage marketing with you:

- We will take steps to limit direct marketing to a reasonable and proportionate level and only send you communications which we believe may be of interest or relevance to you.
- At any time, you can update or correct your personal profile, or change your preferences for the way in which you would like us to communicate with you, including how you receive details of latest offers or news updates from us.
- You can ask us to stop direct marketing at any time you can ask us to stop sending email marketing, by following the “unsubscribe” link you will find on all the email marketing messages, and any online newsletters, we send you. Alternatively, you can contact us by using the contact details specified under paragraph 3 of this Notice to manage your marketing preferences.
- You can change the way your browser manages cookies, which may be used to deliver online advertising, by contacting us for information relating to this please visit our Cookie Notices on our websites.

We recommend you routinely review the privacy notices and preference settings that are available to you on any social media platforms as well as your preferences within your account with us.

## **13. Sharing your personal data**

Insofar we are acting as Controller ( roles are specified in paragraph 2 of this Notice) and it is reasonably necessary for us in delivering our Services to you and for the purposes set out in this Notice, including:

- for the purposes of facilitating and improving our Services ;
- to enable us to carry out and manage our business activities;
- where we are legally obliged to share information;
- if we believe it is necessary in order to investigate, prevent or act regarding illegal activities, fraud, or situations involving potential threats to the rights, property or personal safety of any person, or other such circumstances; and/or
- if we believe it is necessary to investigate, prevent or act regarding situations that involve abuse of our infrastructure or the internet in general (such as voluminous spamming, denial-of-service attacks, or attempts to compromise the security of the website infrastructure), or to otherwise protect our assets or rights,

your personal information may be shared with the below parties:

- entities of the Fortius /OFA Group of companies;

- our business partners, employees, contractors, consultants, agents and professional advisors;
- systems administrators;
- third parties we use or work with to help deliver our Services to you and / or who otherwise carry out services on our behalf or on an outsourced basis to help us manage our business, including (but not limited to):
  - billing services;
  - sales;
  - marketing agencies;
  - analytics providers;
  - document and data storage providers;
  - validation and security service providers;
  - courier services;
  - IT systems or software providers;
  - software development providers;
  - IT support service providers;
  - legal service providers, including GRCI Law for the provision of data protection services;
  - other professional service providers who provide support and advice including in relation to financial / audit, management consultancy, insurance, health and safety, security and intel and whistleblowing / reporting issues;
  - banks payment processing service providers such as Stripe;
  - third-party service providers to assist us with client insight analytics, such as Google Analytics, Hotjar and Crazy Egg (whose privacy policy can be found at <https://www.crazyegg.com/privacy>);
  - third-party platforms to manage and deliver customer relationship management (CRM, Salesforce);
- third parties in the event of any merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our assets (including without limitation in connection with any bankruptcy or similar proceedings);
- other organisations, including credit reference agencies and others for the purposes of fraud/crime protection and investigation.
- courts of law and government, regulatory authorities or other third parties, including the Commission Nationale de L'Informatique et des Libertés (CNIL), to the extent required by law, court order or a decision rendered by a competent public authority and for the purpose of law enforcement;
- other third parties where we have asked for your consent;
- other third parties we use to help us administer our operations, such as website hosts;
- hiring managers, HR and recruitment teams engaged in our recruitment processes; and / or
- administrative and public bodies involved in the assessment process

We will only disclose your personal information outside of the Fortius/OFA Group of companies if disclosure is consistent with a ground for processing on which we rely and doing so is lawful and fair to you.

Specific circumstances in which your personal information may be disclosed to third parties outside of the Fortius and OFA Group of companies include:

- where we consider disclosure is necessary or required by law, to exercise, establish, or defend our legal rights, or to protect your vital interests or those of any other person;
- where we engage third party vendors to perform services on our behalf and these third parties must process personal information to provide their services (as referenced above);

- in connection with a proposed sale, reorganization, or disposal of Fortius or the Fortius group of companies.

We only allow third parties to process your personal information if we are satisfied that they take appropriate measures to protect that information. We also impose contractual obligations on them to ensure they can only use your personal data to provide support and services to us and to you.

We, or the third parties mentioned above, may occasionally also share personal data with:

- our and their external auditors, e.g., in relation to the audit of our or their accounts, in which case the recipient of the information will be bound by confidentiality obligations;
- our and their professional advisors (such as lawyers and other advisors), in which case the recipient of the information will be bound by confidentiality obligations; and
- law enforcement agencies, courts, tribunals, and regulatory bodies to comply with our legal

The specific kind of information we share will depend on your relationship with, and activities with, us and will be shared only to the extent required or permitted by law, and/or with your consent where applicable.

Please note, this Notice does not apply to sharing of personal information by third party providers who may collect personal information from you and may share it with us. In these situations, we strongly advise you to review the applicable the third-party provider's own privacy notice.

#### **14. International data transfers**

In general, we will store your personal data within the European Economic Area ("EEA") and the United Kingdom. However, there may be circumstances where we may send personal data outside of the EEA and the United Kingdom to other members of the Fortius group of companies and / or other members of the Once for All group of companies and / or to third parties, based in other countries for example (but not limited to) for reasons relating to processing and storage by our service providers. For example, we may have cloud storage providers or software development teams with data storage facilities in the US or in other countries outside of the EEA.

Other countries outside of the EEA may have data protection laws that are different, and potentially less protective, than the laws of your own country. However, Fortius and OFA Group will undertake appropriate due diligence and risk assessments prior to transferring your personal information to other jurisdictions and will implement appropriate measures to ensure your personal information has an appropriate level of protection We will ensure that any transfer of your personal data of it is made in accordance with applicable data protection laws and that appropriate security arrangements are in place to protect your personal data, including in terms of the contracts we put in place with the organisation(s) that receives that information.

You can find more details of the protection given to your information when it is transferred overseas by contacting us via the contact details specified in the paragraph 3 above.

#### **15. Retention of Personal Data**

Except as otherwise permitted or required by applicable law or regulation, we will only keep your personal data for as long as is necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting or reporting requirements. This is in line with our data retention policy.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the risk of harm from unauthorised use or disclosure of it, the purposes

for which it is processed, whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may store your personal data for longer periods of time, for instance where we are required to do so in accordance with legal, regulatory, tax, accounting requirements. In specific circumstances we may store your personal data for longer periods of time so that we have an accurate record of your dealings with us in the event of any complaints or challenges, or if we reasonably believe there is a prospect of litigation relating to your personal data or dealings.

Where your personal data is no longer needed, we will ensure that it is disposed of in a secure manner.

## **16. Data Security**

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties that have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

We periodically test the security of our systems to check for vulnerabilities.

## **17. Risk**

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we do not have any control over what happens between your device and the boundary of our information infrastructure. You should be aware of the many information security risks that exist and take appropriate steps to safeguard your own information.

## **18. Encryption**

All information you provide to us is stored encrypted in rest and in transit. Any payment transactions will be managed by our third-party payment processors and will be encrypted.

## **19. Data breach**

We have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

## **20. Changes to your personal information**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us.

## **21. Cookies and other tracking technologies**

Each time you interact with our websites we may, depending on the consent provided and your jurisdiction, automatically collect personal information, including Technical Data which will include data about your device, your browsing actions and patterns, content and Usage Data. We collect this data using cookies, server logs and other similar technologies like pixels, tags and other identifiers in order to remember your preferences, to understand how our websites are used, and to customise our marketing offerings.

Please see more information on Cookie Notice available on our websites.

## **22. Third-party websites, plugins and services links to other websites**

You should be aware that information about your use of the Platform and our websites (including your IP address) may be retained by your ISP (Internet Service Provider) , the hosting provider and any third party that has access to your internet traffic.

Our websites and the Platform may contain links to third-party websites and plugins, for instance a social media login plugin. If you choose to use these websites, plugins, or services, you may disclose your information to those third parties.

We are not responsible for the content or practices of those websites, plugins, or services. The collection use and disclosure of your personal data will be subject to the privacy notices of these third parties and not this Notice. We urge you to read the privacy and cookie notices of the relevant third parties.

### **23. Use of our website / Platform by minors**

We do not target children, and our websites and the Platform is not intended to attract children. Accordingly, our online services that collect personal data are not directed at and should not be accessed by individuals under the age of 18 years, and we request that such individuals do not provide any personal data to us.

Minors must obtain express consent from parents or legal guardians before accessing or providing any personal data. If notified by a parent or guardian, or discovered by other means, that a minor under the age of 18 has provided their personal data to us, we will delete the minor's data that is in our possession.

### **24. Your data protection rights**

Under data protection law you have certain rights in relation to your personal data, for example:

**Request access to your personal information:** You have the right to ask us for a copy of your personal information. This right always applies.

There are some exemptions, which means you may not always receive all the information you ask for. Your right to ask for information in this way is known as making a data subject access request. In most cases, this will be free of charge; however, in some limited circumstances, for example repeated requests for further copies, we may apply an administration fee.

**Request correction of the personal information that we hold about you:** You have the right to ask us to correct information we hold about you which you think is inaccurate. You also have the right to ask us to complete information you think is incomplete. This right always applies.

**Request erasure of your personal information:** You have the right to ask us to delete personal information about you in certain circumstances. This right enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it.

We have the right to refuse to comply with a request for erasure if we are processing the personal information in question for certain specific reasons, including where we process the personal data in question in

order to comply with a legal obligation, or to perform a task in the public interest.

**Object to processing of your personal information:**

You have the right to object to processing in certain circumstances, for example where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

**Request the restriction of processing of your personal information:**

You may ask us to stop processing your personal data in certain circumstances. Where this right applies, we will still hold your personal data but will not process it any further. You are able to ask us to suspend the processing of personal information about you in this way, for example if you want us to establish its accuracy or the reason for processing it.

**Request the transfer of your personal information to another party:**

This right only applies if we are processing information based on your consent or for the performance of a contract and the processing is automated.

The application of these and any other privacy rights you may have depends on applicable data protection law.

It is the responsibility of the Controller to ensure your rights are implemented in an effective manner and therefore to handle your requests concerning your rights. The par (2) above clarifies our role as processor acting on behalf of our Customers. Therefore, when the Customer is acting as the controller to be able to exercise your rights you need to contact the Customer directly (your employer). If you contact us instead, we will liaise with and support the Customer to implement your request in an effective manner.

If you would like more information about your specific rights under data protection law in your jurisdiction and how to exercise those rights, please contact us via the contact details indicated under paragraph 3 above.

Please note, when exercising your rights as set out above, and we are the processor, we need to receive instruction from the controller (our Customer). We may request specific information from you to help us confirm your identity, verify your rights, and respond to your request. Applicable law may allow or require us to deny your request, or we may have destroyed, erased, or made your personal data anonymous in accordance with our record retention obligations and practices.

## **25. How to exercise your data protection rights**

In most circumstances, you do not need to pay any charge for exercising your rights. We have one calendar month to respond to you.

To exercise your rights or get more information about exercising them, please contact the Customer directly and as last instance contact us using the details above and providing us with enough information to identify you.

## **26. Changes to this Notice**

We keep this Notice under regular review to make sure it is up to date and accurate. We encourage you to review this page regularly to identify any updates or changes to our Notice.

## **27. How to complain**

If you have any concerns about our use of your personal data, we hope we can resolve any query or concern you may have in relation to our processing of your personal data and ask that you contact us in the first instance via the contact details listed under paragraph 3 of this Notice.

You can at any time, contact the competent supervisory authorities.

For Belgium :

Autorité de Protection des Données (APD). If you are unhappy with how we process your personal data or if you are unhappy with our response to your complaint using the contact details below:

**Website:** [www.autoriteprotectiondonnees.be](http://www.autoriteprotectiondonnees.be)  
**Address:** **Autorité de Protection des Données**  
Rue de la Presse, 35  
1000 Bruxelles  
**Phone:** +32 (0)2 274 48 00

For France:

Commission Nationale de L'Informatique et des Libertés, (CNIL). If you are unhappy with how we process your personal data or if you are unhappy with our response to your complaint using the contact details below:

**Website:** [www.cnil.fr](http://www.cnil.fr)  
**Address:** **Commission Nationale de l'Informatique et des Libertés**  
3 Place de Fontenoy  
TSA 80715  
75334 PARIS CEDEX 07  
FRANCE  
**Phone:** +33 (0)1.53.73.22.22

For UK:

Information Commissioner's Office (ICO). If you are unhappy with how we process your personal data or if you are unhappy with our response to your complaint using the contact details below:

**Website:** [ico.org.uk/concerns](http://ico.org.uk/concerns).

**Address:**       **Information Commissioner's Office**  
Wycliffe House, Water Ln  
Wilmslow SK9 5AF  
United Kingdom

**Phone:**         0303 123 1113

For Switzerland:

Federal Data Protection and Information Commissioner. If you are unhappy with how we process your personal data or if you are unhappy with our response to your complaint using the contact details below:

**Website:**       <https://www.edoeb.admin.ch>

**Address:**       **Federal Data Protection and Information Commissioner**  
Feldeggweg 1  
CH - 3003 Bern

**Phone:**         058 462 43 95.

For other European countries

You can find the contact details here : [Our Members | European Data Protection Board \(europa.eu\)](#)