

1. Introduction

1.1. The TransferGo entities listed at Schedule 1 (*TransferGo Employers*) ("**TransferGo**", "**we**", "**our**" "**TGO**" or "**us**") provide this notice to you because you are applying to work with us as an employee, worker or contractor.

1.2. This notice sets out the basis on which we will process your personal data. Please read it carefully to understand our practices regarding your personal data and how we will use it.

2. About Us

2.1. TransferGo is the controller of the personal data of prospective employees, workers and contractors, and is subject to applicable data protection laws.

2.2. If you have any questions about this notice or your personal data, or wish to exercise any of your rights as described in this notice or under applicable data protection laws, you can contact Data Protection Officer through dpo@transfergo.com.

3. What types of personal data is processed?

Personal data:

3.1. This notice applies to your "personal data". This is any information relating to you as an identified or identifiable person.

3.2. Within the broad range of information which can be personal data, information revealing the following characteristics are considered "special categories of personal data" in the UK and EEA and are therefore subject to a greater degree of protection:

- physical or mental health;
- racial or ethnic origin;
- political opinions;
- trade union membership;
- religious or philosophical beliefs;
- sexuality or sexual life; and
- genetic and biometric data.

3.3. Outside of the UK and EEA, other types of sensitive personal data, in addition to the "special categories of data" mentioned above, may include:

- social status;
- criminal history;
- membership of a professional or trade association;
- social security numbers;
- bank account information;
- financial data.

4. What personal data we collect

Personal data you give to us

4.1. You may give us personal data about you by filling in forms online, corresponding with us by phone, email, in person, or otherwise, or through a recruitment agency or other third party.

Personal data we collect from you

4.2. The personal data that we collect about you includes, but is not limited to, the following:

- your name;
- home address;
- contact details (such as telephone number and email address);
- date of birth;
- your image or a recording of you, in case You agreed to be recorded or sent this data to TGO;
- copies of your passport, driving license and similar documents;
- education history (including copies of relevant degrees, diplomas or certificates if required), training and professional experience;
- current and past employment details;
- immigration status and work permits;
- languages spoken and level of proficiency;
- test results and scores (including the results of any aptitude or psychometric tests we ask you to undergo);
- criminal record information (where required by laws);

information required to prepare the employment contract;

- other information given in your CV;
- interview notes and recordings;
- diversity information (such as information about your race or ethnicity);
- information about your health, such as any disability you might have.

5. Personal data provided by third parties

5.1. We collect most of the personal data described in Section 4 from you directly.

5.2. However, we may also collect personal data about you from third parties, including:

- existing TGO employees who refer to or nominate you for roles with us;
- governmental authorities (such as local tax authorities, police or court institutions);
- your named referees who you’ve asked to provide us with references;
- any third-party e-recruitment testing partners we work with;
- where allowed by law, third-party background screening providers, credit reference agencies, fraud prevention agencies, sanction screening and criminal convictions screening agencies; and
- where allowed by law, other publicly available sources, such as social media networking sites (such as LinkedIn, Instagram and Twitter).

6. Data relating to criminal convictions and offences

6.1. Where required and allowed by law, we also collect and store personal data relating to criminal convictions and offences. **This data will be collected only after the first round of recruitment.** In cases where we need to identify a lawful basis for such processing, then, depending on local laws, such processing is carried out with your consent, to comply with our legal obligations or on the basis of our legitimate interests (to ensure we hire suitable candidates and not breaching binding requirement of our business scope). **Such process would be run by our service party provider Zinc.** During this process you will be notified about this data collection and processing. This data is only processed where it is necessary for the purposes of:

- complying with or assisting other persons to comply with a regulatory requirement which involves TGO taking steps to establish whether you have committed an unlawful act or been involved in dishonesty, malpractice or other seriously improper conduct;
- preventing or detecting unlawful acts (including fraud);
- any legal proceedings (including prospective legal proceedings);
- obtaining legal advice; or
- establishing, exercising or defending legal rights.

In case you would not accept to be back-ground checked at the certain circumstances, and there are no other ways how to comply with this requirement, we might have to deny the candidacy of you, due to the legally binding obligations to our business nature.

7. What we do with your personal data and our legal basis of processing

7.1. We process your personal data for the reasons listed below. In some countries we require a lawful basis to process your personal data and therefore we have also identified this below.

Purpose of processing	Lawful basis
Assessing your skills, qualifications, and suitability for the role, including taking up references and conducting appropriate background checks.	Legitimate interests (to ensure we hire suitable candidates) or Performance of a contract.
Recruitment processes (including negotiation and communicating with you in relation to your application).	Agreement performance.

<p>Complying with our legal and regulatory obligations, including for the purposes of: preventing illegal working; <ul style="list-style-type: none"> ◆ complying with health and safety obligations; ◆ responding to government statistical monitoring; ◆ assessing fitness and propriety of individuals for ◆ the purpose of relevant regulatory schemes to which we must adhere; considering whether adjustments may need to <ul style="list-style-type: none"> ◆ be made to accommodate an individual with a disability; liaising with relevant tax authorities and other government entities or agencies in relation to attachments of earnings and similar deductions; and communications with public or regulatory bodies. <ul style="list-style-type: none"> ◆ </p>	<p>Compliance with legal obligations.</p>
<p>Recording interviews for quality control purposes and to train our interviewers.</p>	<p>Depending on local laws, either legitimate interests (to monitor the quality of our interviewers) or your consent.</p>
<p>Carrying out equal opportunities monitoring, when applicable.</p>	<p>Consent.</p>
<p>Carrying out analytics in relation to TGO's recruitment practices.</p>	<p>Only anonymized data.</p>
<p>Dealing with any legal disputes involving you or other prospective, current or former employees, workers or contractors.</p>	<p>Legitimate interests (to establish, exercise or defend ourselves against legal claims) or Legal obligations.</p>
<p>Keeping your application data on file so that we can consider you for future roles and opportunities at Revolut which we think you'd be suited to.</p>	<p>Depending on local laws, either legitimate interests (to ensure our recruitment process is as efficient as possible) or your consent. Such data would be kept from 1 month to 1 year. This consent can be withdrawn anytime by contacting recruiting agent in contacts or writing to dpo@transfergo.com</p>
<p>Depending on where you are located, we may take steps to verify your identity during the recruitment process to detect and prevent interview fraud.</p>	<p>Depending on local laws, but your consent or legal obligation.</p>

Special categories of personal data' or 'sensitive personal data'

- 1.1. We process 'special categories of personal data' or 'sensitive personal data' for the purposes of:
- carrying out the obligations we have to exercise both TGO's and your specific rights which are imposed by employment laws;
 - establishing, bringing or defending legal claims; and
 - in the case of personal data about your physical or mental health, to enable TGO to assess your working capacity and take decisions for occupational health purposes.
- In the case of "equal opportunities monitoring",** please note that participation is voluntary and providing this information is optional. Any information you provide will not be accessible or used in the hiring process,
- 7.2. and has no effect on your opportunity for employment.

8. Disclosure of your personal data to third parties

8.1. For the purposes set out in Section 7 above, we may share your personal data with:

- our group companies where necessary to process your application;
- professional advisors (including lawyers, accountants and auditors) where necessary to receive their services;
- legal and regulatory authorities (such as tax authorities) where necessary to comply with our legal obligations;
- **our third party service providers**, including our data hosting service provider (AWS Ireland), background screening check provider (Zinc) and online recruitment testing service providers (Greenhouse, etc.), interview recording tool when you accept the interview to be recorded (Metaview). We also disclose your personal data to third parties where it is in our legitimate interest to do so, including for the following reasons:
 - in the event that we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets;
 - if all or substantially all of our assets are acquired by a third party, in which case personal data held about our applicants will be one of the transferred assets; and
 - if we are under a duty to disclose or share your personal data to comply with any legal obligation.

8.2. Except as set out in this notice, or as required by law, we would not sell your personal data to any third parties.

9. Security of your personal data

9.1. We are committed to ensuring that your personal data is safe and take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this notice.

9.2. Unfortunately, the transmission of personal data through the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your personal data transmitted to or stored on our IT system, and any transmission is at your own risk. Once we have received your personal data, we will use strict procedures and security features to try to prevent unauthorized access.

9.3. If we share your personal data with any third party, we will take all necessary steps to make sure that your personal data is handled lawfully and securely by that third party.

10. How long we keep your personal data

10.1. We will keep your personal data for as long as necessary to fulfil the purposes described in this notice or the terms of any contract that we enter into, or for such longer period as may be required by law. After this, where allowed by laws and this notice, we will erase or anonymize your personal data. If you need any additional information about this, please contact our Data Protection Officer at dpo@transfergo.com

10.2. **Mainly, the retention period set like this:**

- Metaview recorded interview is kept until 2 months;
- If you consented to be reached-out even if the recruitment is unsuccessful at this stage,- the sent information will be kept in GreenHouse up to 1 year. If You did not consented – no data will be processed.
- If You have sent e-mail to TransferGo, this email will be saved up to 30 days.
- Back-ground screen which was made via Zinc platform, due to the employment step confirmation, will be saved up to 2 years.
- If you have come to our Offices, the recording of the CCTV recording image will be saved up to 14 days.

11. Automated decision-making

11.1. We may use automated decision-making in the form of online assessments to help streamline our recruitment processes. These online assessments are mainly designed to assess your competency for the role you have applied for, your working style and / or whether or not you would be suitable for a role with TransferGo. These online assessments will produce a score

based on the responses you provide, which we then use to determine whether or not to progress your application.

11.2. If you are not happy with the outcome of any automated decision we have made, you have the right to challenge this. See the “Exercising Your Rights” section below for more information about how you can do this.

12. Your rights

12.1. Subject to applicable laws in your location, you may have certain rights in relation to your personal data, including the right to:

- access a copy of the personal data which we hold about you;
 - ask us to correct your personal data if you think it's wrong;
 - ask us to delete your personal data in certain circumstances;
 - object to us processing your personal data on the basis of our legitimate interests or another lawful basis in certain circumstances;
 - ask us to restrict how we use your personal data;
 - ask us to transfer personal data to you or another company in a structured, commonly used, machine-readable format;
 - withdraw your consent (where you have previously given us this); and
 - ask us to carry out a human review of an automated decision we make about you.
- to write a complain to Data Inspectorate Authority in case you do believe we have processed data unlawfully.

12.2. Please note that not all of these rights are absolute and we may not be required to comply with your request where exemptions apply under applicable data protection laws. If we are not going to comply, we definitely will reach out and will explain the decision and reasons.

13. Exercising your rights

13.1. You can exercise any of your rights as described in this notice and under data protection laws by contacting TGO’s Data Protection Officer through dpo@transfergo.com.

13.2. Where we have reasonable doubts concerning the identity of the person making the request, we may request additional information necessary to confirm your identity.

13.3. We will endeavor to respond to your request within the time period mandated by applicable law. In the UK and the EEA, this means that we will endeavor to **respond to your request within one month**. Please note, however, that this time period may be extended by a further two months in cases when it is very large and complex. We will definitely inform you regarding such prolonging.

14. International transfers

14.1. Your personal data will be stored on servers located in the United States, UK or EEA.

14.2. Where required by applicable laws, your consent to the transfer of your personal data outside your home country will be obtained as part of your application.

14.3. As an international organization, authorized personnel may access your personal data in any country in which we operate (**see Schedule 1**). Therefore, it may be necessary to transfer your details to members of our group located in countries that may not have equivalent data protection or privacy laws to those which apply in your own country. We may also need to transfer your personal data to third party service providers located in other countries. In case you are interested who exactly gets your data, please contact dpo@transfergo.com and we will review request case-by-case method.

14.4. Regardless of where your personal data is transferred, we will put in place appropriate safeguards to ensure that your personal data is treated securely and in accordance with applicable law. For individuals in the EEA and UK, this usually means entering into Standard Contractual Clauses with the recipients of your data who are located in countries which are not recognized as having adequate data protection laws. More details regarding these safeguards can be obtained from the Data Protection Officer whose details are given above.

15. Complaints

15.1. Please direct any complaints about how TransferGo processes your personal data to our Data Protection Officer. dpo@transfergo.com

15.2. You also have the right to complain to your local data protection authority:

- a list of European Union data protection authorities can be found [here](#);
- the United Kingdom’s data protection authority’s contact details can be found [here](#);

16. Changes

16.1. This notice may be amended by TransferGo at any time. You can always find the latest version of this notice on our website.

Schedule 1
TransferGo Employers details

Location	TransferGo entity	Registration details
United Kingdom	TransferGo Ltd (also as a foreign employer in Belgium, Bulgaria, France, Italy, Romania, Spain, Sweden and Ukraine)	07914165
Lithuania	TransferGo Lithuania UAB and/or GoSystems UAB (also as a foreign employer in Germany, France, Ireland, Netherlands, Poland, Latvia)	TransferGo Lithuania: 304871705 GoSystems: 302928584
Poland	TransferGo Lithuania Sp.Z.o.o.	TAX ID: 1060008081
Turkey	TransferGo Tekoloji A.S., Turkey	