



APPROVED by the Resolutions of the  
Management Board of DTEK GROUP B.V.

A large, thick yellow outline of a stylized letter 'D' that frames the central text. The shape consists of a vertical line on the left and a semi-circular arc on the right.

## **PRIVACY Policy**

Amsterdam  
2025

## Table of contents

<a href="#"><u>1. Introduction and purpose</u></a>	3
<a href="#"><u>2. Terms, abbreviations and definitions</u></a>	3
<a href="#"><u>3. Information about Controller and role responsible for data protection</u></a>	4
<a href="#"><u>4. What Personal data do we process</u></a>	4
<a href="#"><u>5. How we protect Personal data</u></a>	7
<a href="#"><u>6. Transfer of Personal data to a third country</u></a>	7
<a href="#"><u>7. Data subject privacy rights</u></a>	7
<a href="#"><u>8. Final provisions</u></a>	8

## 1. Introduction and purpose

- 1.1** This document sets out the Privacy Policy of DTEK GROUP B.V.
- 1.2** As far the Company determines the purposes and means of the processing of Personal data, GDPR defines the Company as a Controller. This means the Company, as a Controller, has legal responsibility for how we collect and process Personal data.
- 1.3** Data privacy is our priority. We know how important the information about processing Personal data is. This Policy sets out how and why we are processing Personal data, what we do with Personal data, rights of Data subject and ways of their realization. This Policy covers the office premise of the DTEK Group B.V., the website which we use, social media accounts, and other platforms where Data subjects may interact with us.

## 2. Terms, abbreviations and definitions

- 2.1.** For the purposes of this Policy, terms and abbreviations shall have the following meanings:

Terms/Abbreviations	Definitions
<b>CCTV Policy</b>	the CCTV and Security Policy of DTEK GROUP B.V.
<b>Cookie Policy</b>	The Cookie Policy of DTEK GROUP B.V.
<b>Controller</b>	the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal data
<b>Company</b>	DTEK GROUP B.V., a private company with limited liability incorporated under the laws of the Netherlands and registered with the Chamber of Commerce trade register under number 59950293
<b>Data Privacy Manager, DPM</b>	a specified role in the Company or in DTEK Group focused on the data privacy compliance
<b>Data subject</b>	an identified or identifiable natural person to whom Personal data relates
<b>DTEK or DTEK Group</b>	collectively DTEK GROUP B.V. and legal entities directly or indirectly owned or controlled by DTEK GROUP B.V.
<b>DTEK Group Company</b>	any legal entity directly or indirectly owned or controlled by DTEK GROUP B.V.
<b>GDPR</b>	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons 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 or GDPR).
<b>Employee</b>	an employee of DTEK GROUP B.V. or DTEK Group Company
<b>Management board</b>	the management board of DTEK GROUP B.V.

<b>Notice about Personal data</b>	an information document about how the Company processes the Personal data of Employee
<b>Personal data</b>	any information relating to an identified or identifiable natural person ('Data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
<b>Policy</b>	the Privacy Policy of DTEK GROUP B.V.

**2.2.** Terms that are defined in the singular have a corresponding meaning in the plural.

### **3. Information about Controller and role responsible for data protection**

**3.1.** If you have any questions about your Personal data, how we process it, or about this Policy – feel free to contact us:

**Controller**  
DTEK Group B.V.

**Data Privacy Manager**  
E-mail: [dpm@dtek.com](mailto:dpm@dtek.com)

### **4. What Personal data do we process**

**4.1. Personal data from candidates for employment.** From time to time, we are looking for new members for our team. If a candidate wants to join us - we want to know some more information about him. We use Personal data to evaluate and follow-up on candidates' application. During the application process, we will ask the candidate to fill out our questionnaire and provide us with his Curriculum Vitae.

Company is processing Personal data for the purposes, listed below:

<b>Personal data</b>	<b>We use Personal data to</b>
Full name	identify an individual and ensure communication regarding the employment process is accurate and properly relates to him
Date of birth	identify an individual, establish compliance with employment laws
Contact information	have the possibility to contact an individual in relation to employment related matters (for example, to arrange interview)
Emergency contact	contact in the event of exceptional instances
Passport, visa, info about your citizenship	provide information and evidence of compliance with right/permission to work in the Netherlands
Skills, education and qualifications	facilitate the offering of relevant work opportunities and to provide HR-team and potential supervisor with information on skills and qualifications of individual
Curriculum Vitae	make it available to the HR team and potential supervisor as part of finding and offering an individual work that matches his skills, interests and capability and to provide insight on previous roles and experience

We don't process Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and we aren't processing of genetic data, biometric data to uniquely identify you, data concerning your sex life or sexual orientation or data concerning health, except for some limited data explicitly required in accordance with the applicable employment regulations.

Company also offers an opportunity to provide supplementary information and attachments and if the candidate finds it necessary to connect application to his social media accounts (such as LinkedIn or Facebook). Providing this supplementary information is entirely voluntary. Whether the candidate provides this information or not will not affect his application process in any way. Please note that interviews, reference checks and review of information in candidate's social media accounts may be a part of the application process.

Company grounds processing these Personal data on the legal basis of performance of a contract (i.e. to take steps at candidate's request prior to entering an employment contract and/or service agreement). For background checks we base processing of Personal data on the legal basis necessary to comply with a legal obligation.

Since we process Personal data before entering an employment contract with candidate, we will delete all his Personal data regarding your employment if candidate won't join our team. More details are in the Notice about Personal data for job candidates which is provided during application process.

**4.2. Compliance checks.** Company also may collect information connected with candidate's shareholding/participation of legal entities and his politically exposed person status, together with the existence of the restrictive covenants/conditions under his current and/or previous employment contract. We base our processing of these data on the legal basis of legitimate interest to check that there is no conflict of interest in case of candidate's employment or engagement with us.

**4.3. AML and KYC checks for counterparties.** As part of our commitment to comply with applicable legal and regulatory requirements, we may collect and process Personal data from our counterparties to conduct Anti-Money Laundering (AML) and Know Your Customer (KYC) checks. This information is collected to verify the identity of our counterparties, assess potential risks, prevent fraud, and fulfil our obligations under financial and anti-money laundering regulations.

Personal data processed for AML and KYC purposes may include information assisting to define the UBO of the business, including UBO's full name and country of citizenship/permanent residence, date of birth, full name and country of citizenship/permanent residence, date of birth of the trustee (if the ultimate owner is a nominal holder), full name/names of participants or shareholders holding 10% or more of shares, country of their citizenship/residency, date of birth if the counterparty is a legal entity; and first name(s) and surname(s) of the person, birth surname(s) of the Person (if different from the above), date of birth, nationality, National Identification Number, passport number, tax ID number, or other unique identification number (if any) and Place of permanent residence (please provide full home address, including street name; street number; city; post/zip code; country) if counterparty is an individual or a private entrepreneur and relevant documents as required by law. We may share this data with competent authorities or external service providers strictly for compliance and verification purposes.

Data retained for AML and KYC purposes will be stored securely and kept for as long as necessary to fulfil legal obligations. We base our processing of these data on the legal basis of

legal obligations in order to check that there is no violation of applicable financial and anti-money laundering legislation in case of employment and/or engagement.

**4.4. Our Talent bank.** It may happen we can't propose work relevant to candidate's skills and qualifications at that time. Even if we didn't enter an employment contract with an individual at a certain period - we would like not to lose contact with him. For this purpose, we invented our Talent bank. We will process individual's Personal data for the purposes, which we collected from him as it is stated in the Section Personal data from candidates for employment stated above. We base our processing of this data on the legal basis of consent. If an individual gives us his consent for processing data for our Talent bank, we will store his Personal data in our Talent bank for 3 (three) years since we receive data from him. During this period, we may contact him about other existing or future job opportunities. After 3 (three) years we will delete all his Personal data.

**4.5. Whistleblowing and Trust line.** We follow the principles of business ethics outlined in the DTEK Ethics and Business Conduct Code and treats colleagues, partners, stakeholders, clients, suppliers and advisors with honesty and integrity. We support their rights to express concerns about the results of our common goal and report inappropriate actions. If someone decides to submit a report connected with violation of DTEK Code of Ethics and Business Conduct and/or any applicable legislation to the Trustline, his first name, last name, e-mail address, phone number and position might be processed as a part of examination of the violation reports or whistleblowing reports.

Whistleblowing reports, except for the Personal data provided by whistleblower, may be shared with a limited number of third parties to investigate the incident described. Such Personal data will be stored and may be used to communicate with the whistleblower. Such Personal data will be stored in the message database for 36 months after providing the information. The legal basis for the processing of the Personal data that was provided is legitimate interest.

**4.6. Footage from the CCTV.** We want to make our office safe for our guests and Employees, protect the property of our company. To achieve these goals, we use the CCTV system as a complement to other security measures. Our CCTV systems do not infringe on restricted areas (i.e. toilets/restrooms and other similar places). More detailed information about our CCTV system, legal basis of processing, retention period and privacy rights may be found in our CCTV and Security Policy.

**4.7. Information about personal devices.** When an individual connects to our guest Wi-Fi network in our office, we collect IP and MAC (Media Access Control) addresses of his device. We process this info only for technical reasons and store it for 7 (seven) days after which this data is deleted automatically. If you don't want us to process this data, please, use your mobile internet and don't connect to our Wi-Fi network. Also, we may process individual's Personal data, that we gather via Cookie files. Cookie files are small text files that are stored on user's computer or mobile device when he navigates the Internet and that contain a number that allows the user's computer or mobile device to be unequivocally identified, even if the user change locations or IP addresses. We use necessary cookies, without which user would not be able to undertake activities on our website and in addition to necessary cookies, we use optional cookies to improve user experience on our website and make your interactions with us more enjoyable and efficient. These cookies: help us understand how users interact with our website, allowing us to improve its design and content and enable features that enhance usability and personalization, such as remembering your preferences or providing relevant content. While these cookies are not essential for the website's functionality, they contribute

to a better and more tailored browsing experience. We respect your privacy and will only use these cookies with your explicit consent, which you can manage through Cookie settings. More detailed information about Cookie files, that we use, and their retention period you may find in our Cookie Policy.

- 4.8. Information on social media accounts.** We have social media accounts (Facebook, LinkedIn). If an individual comments or otherwise provides information in a public space, we process a record of it and any Personal data included in the comment. For example, this may include comments under our posts through social media, tags or reposts of info on our social media accounts or any other interaction through social media.

## **5. How we protect Personal data**

- 5.1.** We use the complex of organizational and technical measures for Personal data protection. Thus, the Company:
- protects premises, equipment and system software;
  - prevents unauthorized access to Personal data during processing, including transfer via telecommunication networks;
  - ensures effective methods to block, destroy, delete or anonymize Personal data.
- 5.2.** In critical areas, the Company makes periodic assessments of impacts related to Personal data protection, taking into account the risks implied by processing, particularly due to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Personal data transmitted, stored or otherwise processed.
- 5.3.** Pursuant to the Regulation (EU) 2016/679 (General Data Protection Regulation), the Controller also uses methods to pseudonymize, anonymization and encode Personal data collections. The systems and services provide continuous confidentiality, integrity, accessibility and resilience. Technical and organizational measures to provide processing security are regularly tested, assessed and evaluated.

## **6. Transfer of Personal data to a third country**

- 6.1.** We may involve Subsidiaries and/or third parties (as a Data Processor) to process Personal data for the services connected with AML/KYC checks, compliance check, and some other services, including IT, HR and ancillary services. We may transfer Personal data to our Subsidiaries and/or third parties outside the European Economic Area (EEA) under condition that the transfer will occur in accordance with applicable Data Protection Laws. We take reasonable steps to ensure that the Personal data is treated securely (typically through the use of EU-approved Standard Contractual Clauses and related Transfer Impact Assessments).

## **7. Data subject privacy rights**

- 7.1.** Data subject has many rights regarding his/her Personal data. Read more about them below. If you would like to exercise your rights or learn more, feel free to contact us. Please note that some of the rights may not be applicable to your situation.
- 7.2.** We respect individuals' privacy and need to make sure, that the request for realization of Data subject privacy rights was sent by a person, who has a right to do this. For identification and verification, we may send an E-mail and ask for additional information - please, check your E-mail folders (i.e., Inbox, SPAM).
- 7.3.** We won't proceed with this additional information except for identification.
- 7.4.** Please note, that if you don't provide us with such additional information – we can't verify

your identity thus such a request may leave without an answer.

- 7.5.** Upon receipt of the written request, it is referred to the Data Protection Manager who will determine whether realization of your rights is lawful.

**7.6.** Right of access

Data subjects have the right to know what Personal data we process and why. That's why we inform you in advance about our processing activities via this Privacy Policy. If you have any questions, or would you like to learn more about what information we process from you, you are always welcome to contact us, and we will provide you with further information.

**7.7.** Right to rectification

If you suppose we process incorrect information about you, such as your name, address, date of birth, etc., you can ask us to correct this.

**7.8.** Right to erasure / right to be forgotten

You have the right to tell us to permanently erase your data from our records. You can do this for example if you think there's no longer any need for us to keep it. Or, if you previously have given your consent, you can just decide to withdraw it.

**7.9.** Right to restrict the processing activities

You have the right to restrict our processing activities in certain situations. This means we will continue to store your information, but we'll temporarily stop any other processing. Why would you want to do this? For example, if you've asked us to fix incorrect information. In this situation you may want us to stop processing until the information is correct.

**7.10.** Right to data portability

In certain situations, you have the right to ask us to send your Personal data in digital form to you, so that you can forward it to someone else.

**7.11.** Right to object

You have the right to object to the processing of your information, even when we have a legitimate legal reason to process it. You can do this when we process your information based on our legitimate interest, and you believe that your personal interest outweighs ours.

**7.12.** Right to withdraw consent

If we process your Personal data based on your consent, you have the right to withdraw your consent anytime.

**7.13.** Right to contact the Netherlands Data Protection Authority

If you have any complaints, for example, about the way in which we use your data or how we respond to your privacy-related questions, you can submit a complaint to the Netherlands Data Protection Authority, Bezuidenhoutseweg 30, 2594 AV Den Haag, Netherlands, <https://autoriteitpersoonsgegevens.nl>

## **8. Final provisions**

- 8.1.** This Policy is subject to regular review and updating as needed to ensure it continues to reflect the Company's commitment to protect the Personal data and adhere principles of GDPR and the relevant changes in legislation.

- 8.2.** Pursuant to a resolution to that effect and in each case subject to ongoing compliance with applicable law the Management Board may amend or supplement this Policy and allow



temporary deviations from this Policy.

- 8.3.** This Policy shall be governed by and shall be construed in accordance with the laws of the Netherlands.