ENERGO-PRO GROUP

INTERNAL DATA PROTECTION POLICY

2021

ENERGO-PRO

EMPLOYEE (INTERNAL) DATA PROTECTION POLICY

1. Introduction

Our core business is the hydropower sector. We operate hydropower plants in Central and Eastern Europe, the Black Sea and the Caucasus. We are also engaged in the electricity distribution and power trading, operating large-scale distribution grids in Bulgaria and Georgia with more than 2.3 million grid customers.

Our company was established in 1994 in the Czech town of Svitavy, participating in the modernization and rehabilitation of hydropower energy in Central and Eastern Europe in the period of economic transition. The total installed capacity of our power plants is 1,243 MW, while the annual power generation is more than 3.8 TWh.

One part of our group is the Slovenian manufacturer of water turbines, Litostroj Power d.o.o., with projects delivered to more than 60 countries worldwide. Its subsidiary, Litostroj Engineering a.s., registered in the Czech Republic (formerly known as ČKD Blansko Engineering, a.s.), focuses on research, design and engineering works. Litostroj Group also supplies equipment for hydropower plants, including pumped-storage HPP and pumping stations.

2. What this is about

This is the data protection policy of ENERGO-PRO Group[1] ("**we**", "**us**", "**our**"). It must be followed by all employees, contractors, temporary workers, agents, and consultants ("**staff**", or "**you**") working for or with ENERGO-PRO.

We hold personal data about our employees.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) should be consulted before any significant new data processing activity starts to make sure that the relevant compliance steps are addressed.

This policy provides information and guidance that is of general application across all business areas. Why is this important?

If we don't handle personal data responsibly and lawfully, this can have a negative impact on people's trust in our business. Also, our sensitive business information is confidential and needs to be properly protected, otherwise this can mean we lose our competitive advantage, suffer reputational damage or be exposed to legal liabilities.

Importantly, if we don't comply with data protection laws, we can also face massive regulatory fines (of up to the greater of €20 million and 4% of global annual turnover).

3. Definitions

It is important that you understand the following terms:

"**Data protection laws**" means the laws governing the privacy, use and protection of personal data, including the GDPR and any local laws that apply in the country where you work or to the people whose information you use.

"**GDPR**" means the General Data Protection Regulation, which has applied throughout the European Union ("**EU**") from 25 May 2018, and affects organisations established in the EU and also those outside the EU which use personal data of individuals in the EU in certain ways.

[1] The Group includes DK Holding Investments, s.r.o., the sole and direct shareholder of ENERGO-PRO a.s., and all of its direct and indirect subsidiaries.

"**Personal data**" means any information relating to an identified or identifiable natural person (i.e. one who can be identified, directly or indirectly, in particular by reference to an identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person). Identifiers include things such as names, ID numbers, location data and online identifiers.

Examples of the types of people we collect personal data on: current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. Examples of the types of personal data we collect: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, health data, biometrics and CV.

Fully anonymised data (i.e. data from which an individual cannot be identified) and information about deceased people is generally not considered to be personal data.

"**Special category personal data**" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Special category data (sometimes referred to by its former name of "sensitive personal data") requires special protection because of the potential for it to cause prejudice to the person it relates to and so should be strictly controlled in accordance with this policy.

Health data is probably the most typical data you will come across in this category (covering both physical and mental health) and covers whatever reveals information about your health status.

"**Data processing**" means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Pretty much anything you do with personal data is data processing.

"**Data Breaches**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

4. Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms.

We may supplement or amend this policy by additional policies and guidelines from time to time, and we will inform you of material changes.

5. Who is responsible for this policy?

The DPO has overall responsibility for this policy. He or she is responsible for ensuring this policy is adhered to by all staff.

However, getting data protection compliance right is in everyone's interests and is the responsibility of all staff. If you spot a data protection issue (or potential issue), report it and deal with it quickly and always ask for support where you need to.

6. Our procedures

Lawful, fair and transparent processing

We must process personal data lawfully, fairly and transparently in accordance with individuals' rights. This generally means that we should not process personal data unless:

- the processing is:
  - (a) necessary to perform a contract we have with an individual (including an employment contract) or to perform legal obligations that we have; or
  - (b) otherwise necessary for our legitimate interests and is not overridden by the individual's data protection rights; or
- the individual whose details we are processing has consented to this.

Consent must be freely given, specific, informed and unambiguous, and given by a statement or by a clear affirmative action, which shows that the individual agrees to the processing of their personal data. You will need to keep records of consents. If someone withdraws their consent to us processing their information, we will need to stop processing it.

Wherever possible, we should try to ensure the processing is allowed for one of the alternative reasons in the first bullet point above (particularly for employment-related information). In most cases this provision will apply to routine business data processing activities.

Special category personal data

In most cases where we process special category personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work, or if someone is seriously injured and unable to give consent).

Any consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed. The individual will ideally need to respond by a statement in words, and (if possible) which is signed and dated. We use a consent form for specific health purposes. (See Appendix 1.)

Processing for specified purposes

You can't simply collect personal data for "reasons to be determined". You need to ensure personal data is collected only for specified purposes, which you tell the person about. You can't later decide to use that data for something completely different (you would in most cases have to go back and ask for permission to use the data for that different purpose).

Minimising data and accuracy

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive given the purpose for which it was obtained.

You will need to do periodic checks to ensure that personal data that we hold remains accurate and update this as necessary. Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO. Information which is incorrect, misleading, inaccurate or out-of-date data may need to be updated or possibly destroyed – if you're not sure about this then please speak to the DPO.

When creating forms or processes for collecting personal data, you will need to ensure that these capture the minimal data required, and nothing more – any data which is not necessary for the purpose for which it is being or has been collected should not be collected in the first place. We will not process personal data obtained for one purpose for any

unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

7. Data security

We must keep personal data secure against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. This means complying with our security guidelines and policies.

We have an obligation to implement appropriate technical and organisational measures to ensure data remains secure. Depending on the situation it may be appropriate, for example, to:

- limit access rights to data to only specific authorised individuals who need to know it (access controls);
- use de-identified (e.g. anonymised or keycoded) data;
- secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold personal data (and confidential information);
- dispose of personal data securely. Paper documents should be shredded. Floppy disks, CD-ROMs, USBs should be physically destroyed when they are no longer required; or
- use equipment securely. Ensure that third parties such as visitors cannot see personal data on company monitors. Log off from PCs when they are left unattended.

We need to be especially careful with apps and cloud based services. Do not put data into an app or upload it to the cloud without sign-off from the DPO.

You should also always ensure that devices you use to access personal data are encrypted and ensure that proper protections are in place when sharing personal data with others.

Data security is a priority but also an ongoing challenge for our business. We need to ensure that we are regularly testing, assessing and evaluating the effectiveness of the technical and organisational security measures that we use for processing personal data.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our Data Retention Guidelines. (See Appendix 2.)

When destroying or erasing personal data, this must be done in a secure manner.

If it is possible to de-identify the information such that specific individuals cannot be identified from it, we may be able keep this for longer, for example, where this is useful for analytical or statistical purposes.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required, e.g. if your personal circumstances change then please inform the HR Department so that they can update your records.

8. Transferring data internationally

There are restrictions on international transfers of personal data. An international data transfer may happen not only when you send personal data to a recipient who is outside the EEA but also when personal data is accessed or viewed from outside the EEA.

You must not transfer personal data outside the EEA (which includes the EU, Iceland, Liechtenstein and Norway) without first consulting the DPO. Generally, specific contracts or alternative transfer mechanisms will need to be in place before personal data can lawfully be transferred outside the EEA.

You should be particularly careful when looking to use suppliers who are based outside the EEA or who use subcontractors outside the EEA for certain aspects of the services they provide. When using cloud-based services, you will need to check the locations where data is hosted and ensure the requirements relating to international data transfers are complied with.

9. Subject access requests

Under the GDPR, individuals are entitled (subject to certain exceptions) to request access a copy of information held about them. This may include any opinions you and other employees have added to their records. Sometimes these are referred to as "SARs" (which stands for "subject access requests").

Individuals also have rights to request rectification, erasure, restriction, data portability, to object to processing and other rights in relation to automated decision making and profiling.

These various rights are called data subject requests (DSRs). If you receive a DSR, please refer that request immediately to the DPO and follow our DSR procedure at Appendix 3. We may ask you to help us to comply with those requests but you must not reply before contacting the DPO, even to acknowledge the request.

We cannot charge a fee for responding to DSRs, although we can charge for our administrative costs if a request is manifestly unfounded or excessive, particularly if it is repetitive.

None of the DSRs are absolute – there are exceptions and restrictions on the information to which a person is entitled or what they can require an organisation to do in response to a request under data protection laws.

What if you want to make a DSR?

Please contact the DPO if you would like to correct or request information that we hold about you, or exercise any of your other rights outlined above.

10. Reporting data breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- investigate the failure and take remedial steps if necessary; and,
- report the breach to regulatory authorities or the police where it is advisable to do so.

Do not delay in reporting a data breach – time will be critical in bringing the breach under control, plus we have an obligation to report personal data breaches to the relevant regulators (generally within 72 hours). This is very important.

Prevention is the strongest form of defence. If you see anything that is likely to pose a security risk, report it immediately to your line manager.

11. Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided whenever there is a substantial change in the law or our policy and procedure.

Training is provided online.

It will cover:

- the law relating to data protection; and,
- our data protection and related policies and procedures.

Completion of training is compulsory.

The DPO will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or this policy or procedures, please contact the DPO.

12. Monitoring

Everyone must observe this policy. The DPO has overall responsibility for monitoring this policy regularly to make sure it is being adhered to.

13. Failure to comply with this policy

We take compliance with this policy very seriously.

Failure to comply puts both you and the company at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

APPENDIX 1

SPECIAL CATEGORY PERSONAL DATA PROCESSING CONSENT FORM

DECLARATION

The undersigned

_____

(First name, middle name(s) and last name)

Personal Identification Number (or equivalent): _____, in my capacity of:

0 Company employee

_____

0 Spouse, partner living on a family basis, children over 18 years of age of company employee

_____

0 Authorized representative of

_____

0 Other / please describe /:

_____

I DECLARE:

that

I agree

that ENERGO-PRO may process and store the personal data (including my health data) provided by me in documents:

[0 Application for financial support [any applicable health fund];]
[0 Medical documentation described in the application;]
[0 Other / please describe /:]

_____

according to the requirements of:

• Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Regulation (EU) 2016/679); and
• National Data Protection Laws and Regulations,
which I provide in connection with and for the purposes of [purpose, such as financial support for the treatment of a disease that is not paid by the state and/or under any compulsory health insurance scheme.

I am familiar with:
- the purpose and means for processing my personal data (including my health data);
- the voluntary nature of the provision of the personal data;
- the right to access and to correct or delete the data collected and the right to restrict the processing of personal data;
- the right to object to the processing, as well as the right to request the transfer of my personal data to a third party - personal data controller;
- the right to appeal to the National Data Protection Authority [insert link to website] in connection with the processing of my personal data;
- the data protection policy of the companies from the ENERGO-PRO group;
- the contact details of the data protection officer: [insert DPO's email address]; and
- the fact that ENERGO-PRO may need to transfer my personal data (including my health data) worldwide and may use third parties to process my personal data on behalf of ENERGO-PRO.

_____
(I am informed and agree to the processing as described above)

I give my consent as a result of my free will and I am informed that I have the right at any time to refuse to give, in part or in full, my consent and to withdraw an already given consent. Withdrawal of my consent does not affect the lawfulness of the processing based on a consent prior to withdrawal.

[I am informed that in case of refusal (full / partial) it is possible not to continue with the consideration of the application referred to above.]

Date: _____ Declarant: _____
(signature)

Place: _____

* to be completed manually

APPENDIX 2

DATA RETENTION GUIDELINES

Your personal data is stored only for a period that is necessary to achieve the provided purposes.

With regard to the performance of employment relationships, only personal data required by the law shall be processed and shall be kept within the terms set by labour and social security legislation.

In the absence of legal requirements about data retention, the data may be stored for a period of up to 5 years.

APPENDIX 3

DATA SUBJECT REQUESTS

If you would like to submit a request to access, rectify, erase, restrict or object to the processing of Personal Data that you have previously provided to us, or if you would like to submit a request to receive an electronic copy of your Personal Data for the purpose of transmitting it to another company (to the extent this right to data portability is provided to you by applicable law), you may contact us via emails ([insert DPO's email address]). We will respond to your request consistent with applicable law.

Whichever request you are making it should contain a detailed, accurate description of the data in question. When there are reasonable doubts regarding your identity, you might be asked to provide a copy of a document to help us to verify your identity. It can be any suitable document such as your ID card or passport. Should you provide any other documents, personal details such as your name and your address should be clear in order to be able to identify you, while any other data such as a photo or any personal characteristics may be blacked out.

Our use of the information on your identification document is strictly limited: the data will only be used to verify your identity and will not be stored for longer than needed for this purpose. Depending on the nature of your request, please make clear what Personal Data you would like to have changed, whether you would like to have your Personal Data suppressed from our database, or otherwise let us know what limitations you would like to put on our use of your Personal Data. For your protection, we may only implement requests with respect to the Personal Data associated with your account, your email address or other account information or other specific information concerning you, that you use to send us your request, and we may need to verify your identity before implementing your request.

Please note that we may need to retain certain information for recordkeeping purposes. There may also be residual information that will remain within our databases and other records, which will not be removed.

We will comply with your request(s) as soon as reasonably practicable.