Data Protection Policy

We, Camplight Ltd., Identification number: 201875626, with management seat and registered address: 150 Deseti Decemvri str., floor 2, Pleven, 5800, Bulgaria, and Cooperative Camplight Coop., Identification number: 207352038, with management seat and registered address: 150 Deseti Decemvri str., floor 2, Pleven, 5800, Bulgaria, contact details: team@camplight.net (hereinafter collectively referred to as "Camplight Group of Related Legal Entities" or briefly "Camplight Group" and "We"), understand the importance of confidentiality and the protection of your personal data.

Camplight Ltd. and Cooperative Camplight Coop. are related legal entities engaged in uniform and interconnected commercial activities. As such, there may be instances where it is necessary for the two legal entities to process the personal data of the same individuals for the same purposes. Therefore, both organizations have agreed to implement this common data protection policy. This policy applies in situations where the two organizations jointly process the personal data of the same individuals for the same purposes, as well as in cases where each organization processes personal data independently.

I. Data Protection Policy Statement and Definitions

1. Statement

Effective from May 25, 2018, Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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 (the "General Data Protection Regulation" or "GDPR"), came into force, thereby altering the existing legal framework for data protection and free data movement.

As organizations established in the territory of the Republic of Bulgaria and processing data of EU citizens, the Camplight Group has a series of obligations related to the processing of personal data and their free movement in accordance with the GDPR, its implementing acts, and applicable national legislation.

Given this, the Camplight Group will implement this Data Protection Policy ("**Policy**"), which will serve as a minimum standard for the processing of personal data and ensuring their free movement.

The purpose of this Policy is to inform you about how we collect, process, and store your personal data when you interact with us in relation to the goods/services we offer.

Counterparties and all third parties working with or for the Group, who have or may have access to personal data, must read, understand, and commit to complying with this Policy. Counterparties are understood to mean all persons who, in one way or another, are or may be in business relations with the Group, such as, but not limited to, clients, suppliers, partners, contractors, subcontractors, assignors, and others.

This Policy applies to all counterparties, as well as all employees/workers and individuals who have concluded civil contracts with the Group (collectively referred to as "Personnel"), as well as cooperative members and other third parties to whom the Group has provided it in relation to the processing of personal data of data subjects.

The Camplight Group reserves the right to periodically update and amend this Privacy Policy to reflect the current manner in which your personal data is processed.

This Data Protection Policy is published on the Group's website and is accessible to all individuals with whom the Group enters into legal relations.

2. Definitions

Personal Data – Any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, particularly by reference to an identifier such as a name, personal identification number, permanent or current address, IP address, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Controller – In the context of this policy, a data controller is any entity that alone or jointly with others determines the purposes and means of the processing of personal data.

Data Subject – Any living individual whose personal data is held by the Group. This includes customers and counterparties of the Group when their personal data is processed.

Processing – Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Personal Data Breach – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. The controller has the obligation to report personal data breaches to the supervisory authority when the breach is likely to result in a risk to the rights and freedoms of natural persons.

Consent of the Data Subject – Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Third-Party – A natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

II. Obligations and Roles under the Regulation

1. Camplight Group may process personal data both as a data controller (solely determining the purposes and means of processing) and as a data processor, acting on behalf of third-party data controllers.

2. The management of Camplight Group is responsible for developing and promoting best practices in the field of information processing within the Group.

3. Compliance with data protection legislation is the responsibility of all individuals within Camplight Group who process personal data.

III. Data Protection Principles

The processing of personal data must be carried out in accordance with the data protection principles set out in Article 5 of the Regulation. The policies and procedures of the Camplight Group are designed to ensure compliance with these principles.

1. **Personal Data must be processed lawfully, fairly, and transparently**

Lawfully – The Group must identify a lawful basis before processing the relevant personal data. This lawful basis is often referred to as a "ground for processing," such as "consent."

Fairly – To ensure fair processing, the data controller must provide certain information to data subjects, as far as practicable. This applies whether personal data is obtained directly

from data subjects or from other sources. The Regulation increases the requirements for the information available to data subjects, which is covered by the "transparency" requirement.

Transparently – The Regulation includes rules regarding the provision of privacy information to data subjects in Articles 12, 13, and 14. These rules are detailed and specific, emphasizing that privacy notices should be understandable and accessible. Information must be communicated to the data subject in an intelligible form, using clear and plain language.

The specific information that must be provided to the data subject should include, at a minimum:

i. Data identifying the controller and the contact details of the controller and, if applicable, the representative of the controller;

ii. Contact details of the Data Protection Officer (DPO), if the controller determines that it falls within the scope of the mandatory appointment of such a person;

iii. The purposes of the processing for which the personal data are intended, as well as the legal basis for the processing; The period for which the personal data will be stored;

iv. The existence of the following rights - to request access to the data, correction, deletion ("right to be forgotten"), restriction of processing, as well as the right to object to the conditions (or lack thereof) regarding the exercise of these rights;

v. The categories of personal data;

vi. The recipients or categories of recipients of the personal data, where applicable;

vii. Where applicable, whether the administrator intends to transfer personal data to a recipient in a third country and the level of data protection;

viii. The right to complain;

ix. The source of the personal data and, if applicable, whether the data originated from publicly accessible sources; The existence of automated decision-making, including profiling;

x. any additional information necessary to ensure fair processing.

2. Personal data may only be collected for specific, explicitly stated, and legitimate purposes.

Data collected for specific purposes should not be used for a purpose that differs from those for which the data were initially collected (Article 30 of the Regulation).

3. Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

4. Personal data must be accurate and kept up to date at all times, and efforts must be made to ensure that deletion or correction can be carried out promptly, within the limits of the available technical solutions.

i. The data stored by the data administrator must be reviewed and updated as necessary. Data should not be retained if there is a likelihood that it is not accurate.

ii. The management ensures that upon hiring personnel, all staff will be trained on the importance of collecting accurate data and maintaining it.

iii. Also, it is the responsibility of the data subject, or respectively the administrator - in cases where Camplight Group acts as the data processor - to declare that the data transferred for storage by Camplight Group are accurate and current. Completing a form by the data subject/administrator intended for Camplight Group will include a statement that the data contained therein are accurate as of the date of submission.

iv. Employees and counterparties must inform Camplight Group of any changes in circumstances so that personal data records can be updated. It is Camplight Group's responsibility to ensure that any notification regarding changes in circumstances is recorded and appropriate actions are taken.

v. The management of the Group declares that there are appropriate procedures and policies in place to maintain the accuracy and currency of personal data, taking into account the volume of data collected, the speed at which it can change, and other relevant factors.

vi. On an annual basis, the management of the Group will review the retention periods of all personal data processed by Camplight Group, relying on data inventory, and will identify all data no longer required for the registered purpose. This data will be securely destroyed in accordance with the administrator's procedures and rules.

vii. The management of the Group will bring the relevant personal data into compliance with received legitimate requests for data correction within one month from the date of receiving the request, in accordance with the internal procedures for handling requests from data subjects. This period may be extended by an additional two months for complex requests. If Camplight Group decides not to comply with the request, the Group will respond to the data subject to explain its reasons and inform them of their right to lodge a complaint with the supervisory authority and

seek legal remedies.

viii. The management of the Group takes appropriate measures in cases where third-party organizations hold inaccurate or outdated personal data. It informs them that the information is inaccurate or outdated and should not be used for making decisions about individuals. The Group notifies the relevant parties and refers any corrections of personal data to the third parties where necessary.

5. Personal data should be stored in a form that allows the data subject to be identified only for as long as necessary for processing purposes.

i. When personal data are retained beyond the processing date, they will be stored in a suitable manner (minimized, encrypted, pseudonymized) to protect the identity of the data subject in case of a data breach.

ii. Personal data will be kept in accordance with the internal rules for data retention and destruction described in Section IX of the Policy, and once their retention period has expired, they must be securely destroyed according to the procedures outlined in this process.

iii. The management approves any data retention beyond the retention period as per the current Policy and must ensure that the justification is clearly defined and complies with the requirements of data protection legislation. This approval must be in writing.

6. Personal data must be processed in a manner that ensures appropriate security (Article 24, Article 32 of the Regulation).

The Group's management will conduct an impact assessment (risk assessment) when applicable and necessary, taking into account all circumstances related to the management or processing operations of data by Camplight Group.

In assessing the appropriateness of processing, the Group's management considers the potential harm or loss that may be caused to individuals in the event of a security breach, as well as any potential harm to the administrator's reputation, including potential loss of trust.

When assessing appropriate technical measures, the Group's management will consider the following options:

i. Password protection;

ii. Automatic locking of inactive workstations in the network;

iii. Disabling access rights for USB and other portable memory devices;

iv. Antivirus software and firewalls;

v. Role-based access rights, including those for temporarily appointed personnel;

vi. Protection of devices leaving the organization's premises, such as laptops or others;

vii. Security of local and wide area networks;

viii. Privacy-enhancing technologies, such as pseudonymization and anonymization.

When assessing appropriate organizational measures, the Management of the Group will take into account the following:

i. The levels of appropriate training within the Camplight Group;

ii. Measures that account for the reliability of employees (e.g., performance reviews, references, etc.);

iii. Incorporating data protection into employment contracts;

iv. Identification of disciplinary measures for violations related to data processing;

v. Regular staff checks for compliance with relevant security standards;

vi. Control of physical access to electronic and paper-based records;

vii. Adoption of a “clean desk” policy;

viii. Storing paper-based data in lockable filing cabinets;

ix. Limiting the use of portable electronic devices for work purposes outside the workplace;

x. Restricting the use of personal devices by employees at the workplace;

xi. Adopting clear rules for the creation and use of passwords;

xii. Regularly creating backups of personal data and physically storing backup media off-site;

xiii. Imposing contractual obligations on counterparties to undertake appropriate security measures when transferring data outside the EU.

These controls are selected based on the identified risks to personal data, as well as the potential for harm to individuals whose data is being processed.

7. Compliance with the accountability principle.

The Camplight Group will demonstrate compliance with data protection principles by implementing data protection policies, adhering to codes, policies, and contracts, deploying appropriate technical and organizational measures, ensuring data protection by design and

by default, conducting data protection impact assessments, establishing a procedure for personal data breach notifications, and more.

IV. Personal data processed by the Camplight Group.

The Camplight Group processes the personal data of data subjects when they have given consent for the processing of their personal data for one or more specific purposes, or when it is required to process their data by law or for the legitimate interests of the Group, as follows (**Records of processing activities**):

1. **Processing of personal data of the Camplight Group staff::**

Process (description)	Processed personal data	Third parties – recipients of personal data	Retention period of personal data	Method of processing
1. Employee recruitment	Contact details (names, phone numbers, email), education and professional experience data, and other information provided by the candidate.	Employment agency, recruitment service providers, clients	5 years from the date of receipt of the data	By non-automated means – on paper By automated means – computer, hard drive, cloud data storage
2. Signing of employment contracts	Names, Personal Identification Number (EGN), permanent address, IBAN, phone number, email, and legally required data (criminal record, medical condition)	External accounting service providers, National Revenue Agency (NRA), National Social Security Institute (NSSI), Occupational Medicine Service	Until the earlier of the termination of the Group's activities and the transfer of payroll records to the NSSI or 2) the expiration of 50 years.	By non-automated means – on paper By automated means – computer, hard drive, cloud data storage
3. Signing of civil contracts	Names, Personal Identification Number (EGN), permanent address, IBAN, phone number, email	External accounting service providers, National Revenue Agency (NRA), National Social Security Institute (NSSI)	Civil contracts and work delivery protocols – up to 5 years, starting from January 1 of the year following	By non-automated means – on paper By automated means – computer, hard drive, cloud data storage

			the year in which they were issued (for tax and social security control purposes)	
4. Administration of employment relationships/contracts – payment of salaries	Names, IBAN, work experience, income data from other employment/contractual relationships	External accounting service providers, National Revenue Agency (NRA), National Social Security Institute (NSSI)	Until the earlier of 1) the termination of the Group's activities and the transfer of payroll records to NSSI or 2) the expiration of 50 years.	By non-automated means – on paper By automated means – computer, hard drive, cloud data storage
5. Administration of employment relationships/contracts – sick leave and occupational medicine	Names, health condition information from medical certificates when taking leave due to general illness/maternity	Occupational Medicine Service, National Revenue Agency (NRA), National Social Security Institute (NSSI)	Sick leave – 3 years, starting from January 1 of the year following the year in which the medical certificate was issued	By non-automated means – on paper By automated means – computer, hard drive, cloud data storage
6. Administration of employment relationships/contracts – maintaining employment records	Documents related to the employment relationship – orders for appointment, termination of the employment contract, leave requests, etc. Diploma copy – only when the job description requires a specific education or qualification level Criminal background check – only if the law requires proof of	External accounting service providers, National Revenue Agency (NAP), National Social Security Institute (NOI), Employment Agency, and other structures under the Ministry of Labor and Social Policy (MLSP), banks, and payment institutions.	Employment contracts and additional agreements, orders for appointment, reassignment orders, orders for unpaid leave over 30 working days, orders for termination of employment relationships – until the termination of the Group's activities and	By non-automated means – on paper By automated means – computer, hard drive, cloud data storage

	judicial history for the position Medical certificate – only if required by law Photo (on CV and/or diploma)		their submission to NSSI. Unclaimed employment books, register of issued employment books, certificates – 50 years. All other documents and personal data from the file (diploma copy, photo, medical certificate upon hire, phone number, orders other than those specified above, etc.) – until the later of: 1) the termination of the employment relationship or 2) the settlement of relations with the former employee.	

Upon the establishment of business relationships of an employment or civil contract nature, individuals are provided with detailed notices regarding their personal data and/or annexes to the respective contracts are signed concerning their personal data.

2. Processing of personal data of the Group's counterparties:

Process (description)	Personal data processed	Third parties – recipients of personal data	Retention period for personal data	Method of processing
1. Execution and fulfillment of contracts with clients/principals/partners	For legal entities: UIC (Unique Identification Code), name, managing director (MD), contact details, MD's personal identification number (PIN), address, IBAN; data from the Annual Financial Report; General Data Overview (GDO); Annual Activity Report. For individuals: Names, contact details, Personal Identification Number (PIN), address, IBAN. If necessary for the performance of the contract: information on invoices, contracts, personnel, members (information may vary and include full name, email, phone, address, education, profession, and PIN). Other data related to contract performance: third-party databases, reports, registers, and others.	External accountant; payment operation systems; banks; if necessary – competent state authorities.	10 years, starting from January 1 of the year following the year in which the data was provided.	By non-automated means – on paper By automated means – computer, hard drive, cloud data storage
2. Entering into and performing commission agreements with partners	For legal entities: UIC (Unique Identification Code), name, managing director (MD), contact details, MD's personal identification number (PIN), address, IBAN; data from the Annual	External accountant; payment operation systems; banks;	10 years, starting from January 1 of the year following the year in which the data was provided.	By non-automated means – on paper By automated means – computer, hard drive, cloud data storage

	Financial Report; General Data Overview (GDO); Annual Activity Report. For individuals: Names, contact details, Personal Identification Number (PIN), address, IBAN. If necessary for the performance of the contract: information on invoices, contracts, personnel, members (information may vary and include full name, email, phone, address, education, profession, and PIN). Other data related to contract performance: third-party databases, reports, registers, and other relevant documents.	if necessary – competent state authorities.		
3. Entering into and performing contracts with contractors/subcontractors	For legal entities: UIC (Unique Identification Code), name, managing director (MD), contact details, MD's personal identification number (PIN), address, IBAN; data from the Annual Financial Report; General Data Overview (GDO); Annual Activity Report. For individuals: Names, contact details, Personal Identification Number (PIN), address, IBAN.	External accountant; payment operation systems; banks; if necessary – competent state authorities.	10 years, starting from January 1 of the year following the year in which the data was provided.	By non-automated means – on paper By automated means – computer, hard drive, cloud data storage

	If necessary for the performance of the contract: information on invoices, contracts, personnel, members (information may vary and include full name, email, phone, address, education, profession, and PIN). Other data related to contract performance: third-party databases, reports, registers, and other relevant documents.			
4. Responding to inquiries, questions, and comments via Contact Form on the website, social media, email, and phone calls.	The extent of sharing personal data is at the discretion of the user/client – Names, phone numbers, email, and other relevant information.	Data is not provided to third parties unless the Group is legally obligated to do so.	Up to 6 months	By non-automated means – on paper By automated means – computer, hard drive, cloud data storage

3. Processing of personal data of member-cooperators:

Process (description)	Personal data processed	Third parties – recipients of personal data	Retention period for personal data	Method of processing
1. Acceptance of a new member – filling out an online form/application and approval by the	Contact details (name, phone number, email), data on education and professional experience, and other information provided by the applicant.	Data is not provided to third parties unless the cooperative is legally obligated to do so.	Until the termination of membership	Through automated means – computer, on hard drive, in cloud server

Process (description)	Personal data processed	Third parties – recipients of personal data	Retention period for personal data	Method of processing
Board of Directors				
2. Conducting General Meetings and meetings of the governing bodies of the Cooperative – preparation of invitations and minutes.	Names, signature, Personal Identification Number (PIN) when authorizing, emails, statements/proposals made.	TRRYULNC (in case of changes in circumstances and announcement of acts voted at the General Meeting)	Storing invitations and minutes from General Meetings and Board Meetings – until the termination of the Cooperative	Through non-automated means – on paper Through automated means – computer, on hard drive, in cloud server
3. Events	Names, photos, videos from events	They may be accessible through the internet and social media, as well as the Cooperative's web pages.	Until the termination of the Cooperative	Through automated means – computer, on hard drive, in cloud server
4. Election of members of the Board of Directors and the Supervisory Board	Names, Personal Identification Number (PIN), contact information, photos	TRRYULNC, NRA (only personal data of the Chairman), banks (only personal data of the Chairman)	Minutes – until the termination of the Cooperative, Contact information and photos – until the end of the mandate in the Board/Supervisory Board or the termination of membership	Through non-automated means – on paper Through automated means – computer, on hard drive, in cloud server
5. Maintaining a database of members	Names, email, phone number, date of birth, city of birth and current city, gender, photos, high school, university, major, other training, languages, current employer, current	Data is not provided to third parties unless the Cooperative is legally	Until the termination of membership	Through automated means – computer, on hard drive, in cloud server

Process (description)	Personal data processed	Third parties – recipients of personal data	Retention period for personal data	Method of processing
	job position, previous jobs, professional interests, personal interests, dates of payment and/or receipt of contributions	obligated to do so.		

3. Grounds and Purposes of Personal Data Processing

Processing of your personal data for these purposes is, in most cases, necessary for the conclusion and performance of a contract between you and the Group (including contracts concluded remotely, as well as for applicable unnamed contracts, mandate contracts, work contracts, supply contracts, brokerage contracts, purchase and sale contracts, and others). Furthermore, processing is required according to applicable legal provisions in the territory of the Republic of Bulgaria, including tax and accounting legislation, to achieve these purposes.

- **Marketing**

Our goal is for you to always be informed about all upcoming events and the best offers regarding the services organized or offered by the Group. In this regard, we may send you all kinds of messages through electronic communication channels that contain general and thematic information. We always ensure that this processing is carried out in strict compliance with your rights and freedoms and that the decisions made in connection with them do not have any legal consequences for you.

- **Protection of Our Legitimate Interests**

There may be cases where it is necessary for us to use or transmit information to protect the rights of the Group. These may include:

i. Measures to protect the Group's website against cyberattacks;
ii. Measures for timely prevention and detection of fraud attempts, including the transmission of information to competent public authorities;
iii. Measures for managing various other risks.

The primary reason for this type of processing is the legitimate interests of the Group related to the protection of its activities. We ensure that all measures we take consider both our interests and your fundamental rights and freedoms.

Currently, we store and process your personal data within the territory of the Republic of Bulgaria. However, there is a possibility that some of your data may be transferred to entities located within the European Union or outside it.

V. Data Subject Rights

1. Each data subject has the following rights regarding the processing of data, as well as the data recorded about them:

i. To make requests for confirmation of whether personal data related to them is being processed, and if so, to gain access to the data, as well as information on who the recipients of this data are;

ii. To request a copy of their personal data from the controller;

iii. To request the controller to correct personal data when it is inaccurate or no longer up-to-date;

iv. To request the controller to delete personal data (the right "to be forgotten");

v. To request the controller to restrict the processing of personal data, in which case the data will be only stored but not otherwise processed;

vi. To object to the processing of their personal data;

vii. To object to the processing of their personal data for the purposes of direct marketing.

viii. To complain with a supervisory authority if they believe that any provision of the Regulation has been violated;

ix. To request and receive their personal data in a structured, widely used, and machine-readable format;

x. To withdraw their consent to the processing of personal data at any time with a separate request made to the controller;

xi. Not to be subject to automated decision-making that significantly affects them, without the possibility of human intervention;

xii. To object to automated profiling that occurs without their consent.

2. The Camplight Group provides conditions that ensure the exercise of these rights by the data subject:

i. Data subjects can make requests for data access;

ii. Data subjects have the right to file complaints with the Camplight Group regarding the processing of their personal data.

VI. Consent

1. By "consent," the Camplight Group will understand any freely given, specific, informed, and unambiguous indication of the data subject's wishes, by a statement or by a clear affirmative action, which signifies agreement to the processing of personal data related to them. The data subject may withdraw their consent at any time.

2. The Camplight Group understands "consent" to mean only those cases where the data subject has been fully informed about the planned processing and has given their consent freely without being subjected to pressure. Consent obtained under pressure or based on misleading information will not constitute a valid basis for processing personal data.

3. Consent cannot be inferred from the absence of a response to a communication sent to the data subject. There must be active communication between the controller and the data subject for consent to be valid. The controller must be able to demonstrate that consent was obtained for the processing activities.

4. In most cases, consent for the processing of personal data and special categories of data is routinely obtained by the Camplight Group using standard consent documents, such as when a new client signs a contract or during the hiring of new personnel, etc.

VII. Data Security

1. All employees/workers are responsible for ensuring the security of the data they are responsible for and that the Camplight Group holds, ensuring that the data is stored securely and not disclosed under any circumstances to third parties unless the Camplight Group has granted such rights to that third party through a contract/confidentiality clause.

2. All personal data must be accessible only to those who need it, and access can only be granted in accordance with established access control rules. All personal data must be treated with the highest security and must be stored:

i. in a separate room with controlled access; and/or in a locked cabinet or file drawer; and/or

ii. if computerized, protected with a password in accordance with internal requirements specified in the organizational and technical measures for controlling access to information (such as access control rules); and/or

iii. stored on portable computer media that are protected in accordance with organizational and technical measures for controlling access to information.

3. An organization must be established to ensure that computer screens and terminals

cannot be viewed by anyone other than authorized employees/workers of the Camplight Group. All employees/workers are required to be trained and to accept the relevant contractual clauses/declaration/notification regarding the collection, processing, and storage of personal data.

4. Paper records should not be left where they can be accessed by unauthorized persons and cannot be removed from designated office premises without explicit permission. As soon as paper documents are no longer needed for ongoing work, they must be destroyed in accordance with the internal rules established in Section IX of this policy.

VIII. Data Disclosure

1. The Camplight Group ensures that personal data is not disclosed to unauthorized third parties, which includes family members, friends, government bodies, or even investigative entities if there is reasonable doubt that the data is not required by established procedures. All employees/workers must exercise caution when asked to disclose stored personal data about another individual to a third party. It is important to consider whether the disclosure of the information is related to the operational needs of the organization.

Employees receive specialized training and periodic briefings to avoid the risk of such violations.

2. All requests from third parties for data provision must be supported by appropriate documentation, and all such data disclosures must be specifically authorized by the Manager of the Group.

Recipients of Your Personal Data

The Group is committed to applying the highest standards of ethical and legal practices in all its activities, including the protection of the personal data of all website users. Except in the cases listed below, we will neither disclose nor allow any person outside the Group to have access to or use your personal information.

Depending on the specifics of each individual case, we may transfer or provide access to some of your personal data to the following categories of recipients:

i. payment/banking service providers;
ii. courier service providers;
iii. external accounting firms;
iv. subcontractors of services offered by the Group;
v. and other categories of persons in connection with the conclusion and execution of contracts (including oral and informal ones) between you and the Group.

We guarantee that access to your data by private entities - third parties is conducted in accordance with legal provisions on the protection of personal data and information confidentiality, based on contracts signed with them. These third parties are obligated to protect the confidentiality and security of your personal information and data. They are not authorized to use, disclose, or alter this information in any way other than for the purpose of performing the services assigned by the Group.

If we are legally obliged or if it is necessary to protect our legitimate interests, we have the right to disclose certain personal data to public authorities.

IX. Data Storage and Destruction

1. The Camplight Group does not store personal data in a form that allows the identification of data subjects for a longer period than is necessary in relation to the purposes for which the data was collected.

2. The Camplight Group may store data for longer periods only if the personal data will be processed for archiving purposes, in the public interest, for scientific or historical research, or for statistical purposes and only by implementing appropriate technical and organizational measures to ensure the rights and freedoms of the data subject.

3. The retention period for each category of personal data is specified in this Policy.

4. Personal data is destroyed securely, in accordance with the requirements of Article 5, paragraph 1(e) of the Regulation, by applying appropriate technical or organizational measures against accidental loss, destruction, or damage ("integrity and confidentiality").

5. Once the necessity for processing the respective category of personal data no longer exists, the Camplight Group takes steps to destroy the data in accordance with these rules.

6. All personal data stored on paper is destroyed in the Camplight Group's office using a shredding machine (shredder). If such a machine is not available at the time when the obligation to destroy arises, the data is destroyed by cutting with scissors, and the person responsible for the destruction must ensure that the data cannot be restored after cutting. When other data that is still being processed by the Group for a specific legal basis is contained on the respective paper medium, the unnecessary data is deleted from the paper medium using means that prevent its restoration.

7. Data stored in the form of electronic messages (emails) is destroyed by permanent deletion.

8. Personal data stored in electronic form is deleted in a way that does not allow its restoration.

9. After the destruction of personal data, the person who carried out the destruction issues a specific protocol, which must contain information regarding the category of personal data, the form in which the data was stored, the basis for the destruction, the method of secure destruction, the date of destruction, and the name and signature of the person who carried out the destruction.

X. Data Processing Register (Data Inventory)

1. The Camplight Group uses a data inventory process as part of its approach to addressing risks and opportunities in the process of ensuring compliance with the Regulation where applicable. In the data inventory process within the Camplight Group and its data workflow, the following are identified:

- Business processes that use personal data;
- Sources of personal data;
- The number of data subjects;
- Description of the categories of personal data and elements within each category;
- Processing activities;
- Purposes for which the personal data are intended;
- The legal basis for processing;
- Recipients or categories of recipients of personal data;
- Main systems and storage locations;
- All personal data subject to transfers outside the EU;
- Retention and deletion periods.

2. The Camplight Group is aware of the risks associated with the processing of certain types of personal data.

3. The Camplight Group assesses the level of risk to individuals related to the processing of their personal data. Data protection impact assessments are conducted in relation to the processing of personal data by the Group and in relation to processing undertaken by other organizations on behalf of the Group.

4. The Camplight Group manages all risks identified by the impact assessment to reduce the likelihood of non-compliance with these regulations. When a type of processing could result in a high risk to the rights and freedoms of individuals, especially by using new technologies and considering the nature, scope, context, and purposes of the processing, the Camplight Group should conduct an impact assessment of the intended processing operations on personal data protection before proceeding with the processing. A single impact assessment may address a set of similar processing operations that pose similar

high risks.

XI. Complaints

You have the legal right to lodge a complaint with the local supervisory authority regarding the processing of your personal data. In the territory of the Republic of Bulgaria, the contact details for the supervisory data protection authority are as follows:

Commission for Personal Data Protection
Address: 2 Tsvetan Lazarov Blvd, Sofia, Bulgaria
Phone: +359 2 915 3580; Fax: +359 2 915 3525
Email: kzld@cpdp.bg
Website: http://www.cpdp.bg/

Without limiting in any way your legal right to contact the supervisory authority at any time, we kindly ask you to contact us first, and we promise to make every effort to resolve any issues by mutual agreement through the following contact methods:

Address: 150 Deseti Dekemvri St, 2nd Floor, Pleven 5800
Email: margarita@camplight.net
Contact Person: Margarita Hristova

This Data Protection Policy was approved by the Director of "Camplight" Ltd. on May 25, 2018.

The policy was updated on April 20, 2023, and approved by the Director of "Camplight" Ltd. and the Chairman of the "Camplight Coop" Cooperative.

Find the Bulgarian version of the policy here: Политика за защита на личните данни на Camplight Group