Privacy Policy

GDPR Documentation Series

PHOENIXPRO

REDEFINING SUCCESS

Prepared by: PhoenixPro – v04
November 2023

Table of Contents

A. Overview

On the 25th of May 2018, the new European data privacy law, known as the General Data Protection Regulation ("GDPR"), has come into force. GDPR defines a specific framework and set of rules for the protection of individuals within the European Economic Area (EEA) with regard to the processing of their personal data.

Any physical or legal person, be it an individual, a company or an organization that collects, stores, manipulates or otherwise processes personal data (hereafter collectively referred to as "processing") is affected, and is required to adopt appropriate technical and organizational measures that make such processing compliant to the provisions of the GDPR. GDPR affects therefore any physical or legal person or body who performs processing irrespective if they are established within or outside the European Union, so long as such physical or legal persons perform processing of personal data for individuals who are in the European Union.

This Privacy Policy has been prepared by PHOENIXPRO, with the objective of assisting our customers, employees, vendors, partners and all other interested parties that may be affected, gain an understanding of the measures we have adopted and operate as part of our own GDPR compliance program and practices. When we mention "PHOENIXPRO" "we", "us" or "our" in this Privacy Policy, we are referring to PHOENIXPRO Ltd, the entity responsible for processing your data.

B. PHOENIXPRO as a Data Controller or Data Processor

In running our business, PHOENIXPRO is a Data Controller or a Data Processor under the GDPR, with possible access to, and processing of personal data of, our employees and our suppliers as well as our customers' Ultimate Beneficial Owners (UBOs), directors and officers, employees, clients and / or suppliers. PHOENIXPRO is committed to performing such processing in transparent and fair ways, based on processes which are private by design and using appropriate technical and organizational measures in support of security and privacy objectives. This commitment is applicable throughout the lifecycle of personal data processing, including during collection, transmission, use and storage (collectively referred to as "processing").

PHOENIXPRO also commits to taking all reasonable steps to ensure that personal data processing is based on a valid legal basis [1]. When PHOENIXPRO is the Data Processor, this commitment typically means that we rely on the Data Controller in each case, to establish a valid legal basis [1] for the processing we perform in that capacity. We also depend on the Data Controllers to notify us in a timely manner when any changes to the status of such legal bases occur. In certain other cases, the processing we perform is dictated by legislation or may be based on our legitimate interests, especially those which emanate from our professional obligations and responsibilities and / or other regulatory frameworks subject to which we perform our work.

[1] See definitions in the Glossary to this Privacy Policy

C. What is the Basis for Processing Your Personal Data

In accordance with Article 6 of the GDPR, personal data processing is lawful if at least one of the processing bases described below applies:

- the existence of evidenced consent of the data subject (i.e. the physical living person), whose personal data is processed
- processing is necessary in order to enter into a contract to which the data subject is a contractual party or to take action at the request of the data subject before or after a contract is entered into force
- processing is necessary to comply with a statutory obligation of the Data Controller or Data Processor as relevant
- processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or Data Processor as relevant, unless such interest overrides the interest or fundamental rights and freedoms of the data subject who require the protection of personal data, in particular if the subject of the data is a child
- processing is necessary to safeguard the vital interest of the data subject or other natural person
- processing is necessary for the performance of an obligation performed in the public interest or in the exercise of public authority assigned to the Company.

Based on the above, PHOENIXPRO seeks to ensure that each type of personal data processing we perform is supported by one or more of the above legal bases. With very few exceptions, the legal bases applicable to our operational routines and the resulting personal data processing we conduct are those described in the first four bullets.

D. How Do we Collect Personal Data

In most cases, we receive personal information for the data subjects from 3rd party sources. Key examples include receiving personal data as follows:

- from our customers (or other colleagues of the respective data subjects) for their shareholders, Directors, Officers, customers, employees, suppliers and other collaborators
- references from previous employers during an employment application process
- lawful 3rd party databases during Know Your Customer (KYC) checks we may perform, and other lawful services of similar nature.

In other cases, we receive the personal data directly from the affected individual (i.e. the “data subject”). Typically, such personal data is requested of the data subject when we initiate our relationship, or in some cases at a later stage, after we commence interacting with each other. There are various means we may accept and use for receiving personal data including paper-based forms, electronic self-service functions (e.g. in a website), or through email communications or physical exchange of contact information (such as a business card).

We may also collect personal data via automated means when data subjects interact with resources we provide (websites logs, email submission tools, etc.). We may also enhance the personal information we process about data subjects, as a result of the interactions and / or transactions between the data subjects and PHOENIXPRO.

E. Why we Process Personal Data

We describe below the key ways we use personal information, and the legal bases of processing on which we rely for such processing. We have also identified what our legitimate interests are where appropriate.

In general terms, we use personal information we collect to help PHOENIXPRO deliver our services for one or more data subject categories, as those are tabulated below (not a definitive or exhaustive list):

#	Business Relationship	Type of Processed Personal Data	Legal Basis
a.	Customers	The information listed below relates to business-to-business relationships between PHOENIXPRO and its customers, which includes, results or requires personal data processing of Directors, Officers, employees, suppliers and other individuals of PHOENIXPRO's customers involved in the relationship, as well as other physical persons who have responsibility for managing or executing dealings between the two parties. • Identify and position / role information • Location information (physical address and electronic location data) • Business eMail address and phone numbers • Mobile phone numbers (corporate or personal) • Authority to place orders, make financial inquiries, execute financial transactions, etc. • Financial data including invoices, payments, due dates, etc. • Payroll and related records	Contract Legislation Legitimate Interest
b.	Applicants	• CV information • Contact details • Previous employment records • Referee • Clear Police / Criminal Record • Work permit information • Skills & Professional and Academic Achievements (e.g. languages, academic degrees	Consent Legitimate Interest (for application information voluntarily submitted by the applicant to us, unsolicited by PHOENIXPRO
c.	Employees, Contractors & Workers	• "Master Data" [full name, ID, Social Security number, address, marital status, children, age, gender, personal emails] • "Recruitment Data" [academic records, experience, previous employers, references] • Evaluation & Performance Information [salary, appraisals, promotions, disciplinary data, complaints and resulting investigations, appeals against HR decisions] • Occupational data [languages, special skills, driver license] • Operational data [sales, locations of travel, training records, leave of absence, timesheets / arrival and departure times, passports and IDs in support of business travel arrangements] • Financial data [payroll, payroll-related, life insurance details, family status, bank account details]	Contract

#	Business Relationship	Type of Processed Personal Data	Legal Basis
d.	Former Employees, Contractors and Workers	For former employees, contractors or workers, the personal data types listed in (b) above are processed with the following differences: • Financial data are kept for a period of 12 years after termination or resignation, for tax and regulatory purposes • All other data are kept for a period of 3 years after resignation or termination for the purposes of archiving and / or providing references	Employment and Social Insurance Legislation Employment / Work Contracts
e.	Suppliers	The information listed below relates to business to business relationships between PHOENIXPRO and its suppliers, which includes, results or requires personal data processing of Directors, Officers and personnel of the PHOENIXPRO's suppliers' personnel involved in the relationship, as well as other physical persons who have responsibility for managing or executing dealings between the two parties. • Identify and position / role information • Location information (physical address and electronic location data) • Business eMail address and phone numbers • Mobile phone numbers (corporate or personal) • Authority to place orders, make financial inquiries, execute financial transactions, etc. • Financial data including invoices, payments, due dates, etc.	Contract Legitimate Interest
f.	Event Attendees	• Full name • Employer • Work position and title • Work / office location • Work and Mobile Phone numbers • eMail address (work and / or personal) • Photos and images	Consent
g.	General Public	• Full name, eMail, phone numbers, employer, title (for cases where you initiate an electronic communication and / or correspondence with us) • Photos and images of you from CCTV cameras we operate at our office locations	Legitimate Interest
h.	Website Users	• Full name • Gender • eMail address (business or personal) • Mobile, and work phone numbers • Electronic identifiers such as IP addresses	Consent

Kindly be aware that your personal data may be processed based on more than one lawful purposes. If you need more information as to the specific legal basis on which we are relying to process your personal data, please send us your specific request to dpo@phoenixpro.com .

F. How Long we Keep your Personal Data

Personal data may be maintained by us in physical and / or electronic form and be processed in ways designed to respect the principles of purpose limitation; data minimization; data accuracy; integrity and confidentiality; and retention limitation.

Specifically with regards to retention, the technical and organizational measures operated by PHOENIXPRO are designed to result in personal data being kept only for as long as required to fulfil our statutory, professional and / or regulatory obligations, and – if for longer periods - in accordance with the provisions of the specific legal basis of processing relating to each category of affected persons.

At the end of the retention periods applicable in each case, defined operational processes or routines shall result in personal data being deleted or destroyed in controlled ways, in electronic and physical form, as appropriate. In some circumstances we may anonymise your personal information (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

G. Sharing of Personal Data

Within PHOENIXPRO, your personal information can be accessed by or may be disclosed internally on a need-to-know basis, based on user access rights management processes.

Your personal information may also be accessible and / or accessed by third parties, including suppliers and advisers, as those are outlined below. When this happens, we take specific measures and steps to protect such information, as described in more detail in section "*SUB-PROCESSORS TO PHOENIXPRO*" of this Privacy Policy. In summary, such measures and steps include requiring all such 3rd parties to respect the security of your personal information and to treat it in accordance with the law. We do not allow our 3rd party service providers to use your personal information for their own purposes and only permit them to process your personal information for specified purposes and in accordance with our instructions. The types of 3rd parties that may typically be involved in processing of your personal data include:

- Service providers acting as Data Processors based in the EEA who provide IT, system administration services, marketing and payment providers in order to service you, interact with you and communicate with you.

- Professional advisers including lawyers, bankers, auditors and insurers based in the EEA who provide consultancy, banking, legal, insurance and accounting services.

- Tax and Customs authorities, regulators, law enforcement bodies and other authorities acting as processors or joint controllers based in the EEA who have the right to require reporting of processing activities in certain circumstances and otherwise in defense of legal claims.

In addition, there are circumstances where we may need to disclose your personal information to 3rd parties, to help manage our business and deliver our services. In this context, we may disclose your personal information:

- to 3rd parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If such a change happens to our business, then the new owners may use your personal information in the same way as set out in this Privacy Policy

- to 3rd parties when we are under a duty to disclose or share your personal information in order to comply with any legal or regulatory obligation, or in order to enforce or apply our legal rights, in which case we may share your personal information with our regulators and law enforcement agencies in the EEA, or to our

legal advisers and

- when it is necessary in order to protect the rights, property, or safety of PHOENIXPRO or any member of PHOENIXPRO of companies, in which case we may disclose your personal information to our legal advisers and other professional services firms.

We may also disclose your personal data to national authorities and government bodies if legislation allows or compels us to do so.

H. Technical & Organisational Measures Protecting Personal Data

GDPR imposes obligations to Data Controllers and Data Processors which are in several cases dependent upon consistent implementation of relevant measures and controls across their own operations as well as those of their Data Processors. Our policy is to process personal data with due regard to the security, privacy and protection of the data we receive, store and process. This privacy policy explains the types of such technical and organizational measures that we employ so as to enhance the level of protection of personal data that we process. These measures are also designed to maximise the control over privacy in accordance to GDPR and have the objective of providing a level of security that is appropriate to the related risks.

- As part of our overall data protection framework, PHOENIXPRO has appointed a Data Protection Officer (DPO), in accordance with the requirements of GDPR. Our DPO can be contacted at dpo@phoenixpro.com.

- All our personnel, periodically observe GDPR-specific awareness sessions so as to maintain the currency of their understanding of GDPR and how it may impact our various operations that affect personal data we process.

- We support the implementation of 3rd party entities' (such as our customers, suppliers) lawfully issued instructions to us, in relation to data subjects for whom such 3rd party entities are Data Controllers, exercising their rights under GDPR, so long as such instructions do not come in conflict with our own legal, professional or regulatory obligations. In such cases, we shall seek to notify the 3rd party entity of the options available to them.

- We seek to ensure that 3rd parties who support PHOENIXPRO operations or systems or who are otherwise involved in our personal data processing operations (including those of our own customers or other affected persons), have and operate necessary technical and organizational measures for protecting the security and privacy of personal data.

- Our Incident Response Management and breach notification procedures, are designed to include escalation of identified incidents to our Data Protection Officer, who is authorized and trained to involve customer handling executives when such incidents involve personal data of one or more of PHOENIXPRO affected entities and / or persons.

- Our processes are designed not to allow cross-border data transfers of personal information to which we have access and / or process during any customer engagement. If such cross-border data transfers are necessary, we shall seek to ensure that a valid lawful basis for such transfers evidently exists, in accordance with GDPR.

- Our recruitment and ongoing personnel training and development, as well as the evaluation and disciplinary processes we operate, are designed to promote and maintain a high standard of professional ethics and competency at all levels of PHOENIXPRO, which is in line with industry standards and our professional and legal responsibilities.

- In addition, PHOENIXPRO operates several complementary technical and organisational measures, designed to protect the privacy of personal information that we collect, store and process. Such measures include logical access controls and user rights management with the objective of minimising access to personal (and other PHOENIXPRO) information and data, only to authorised PHOENIXPRO personnel. We also utilise user access credentials management with enforced frequent changes, password complexity and maximum / minimum lengths, restrictions on reuse of same passwords, etc., complemented by a structured process for periodic review and confirmation of continued business need to such personal data.

- Furthermore, PHOENIXPRO uses purpose-specific technologies and tools (such as firewalls, intrusion prevention, mail security gateways, etc.), all designed to monitor and manage the security of its electronic perimeter. PHOENIXPRO also has in place an active and ongoing patch management program for addressing newly released threats, and benefits from the use of endpoint malware protection at laptop, servers and desktop level. Finally, we also employ endpoint encryption, to protect against privacy risks in cases of hardware theft or loss.

I. Sub-Processors to PHOENIXPRO

PHOENIXPRO utilizes a very limited number of 3rd parties as part of its business operations and routines. Such 3rd parties include legal and / or physical persons who provide services and / or products relating to technology, marketing, legal and other areas which may have an impact on personal data processing (including processing as specified in this Privacy Policy).

When necessary in the context of such personal data processing, our selection process and criteria for cooperation with 3rd parties (suppliers, vendors or other advisors), incorporates consideration and evaluation of those 3rd parties' level of GDPR readiness and compliance. In this respect, we seek to ensure that 3rd parties who support PHOENIXPRO operations or systems or who are otherwise involved in our personal data processing operations, have and operate necessary technical and organizational measures for protecting the security and privacy of personal data.

J. Your Rights

Individuals whose data are processed, have defined rights under the GDPR. Specifically, GDPR requires Data Controllers and Data Processors to implement the necessary processes and mechanisms in support of data subjects' exercising the following rights, the exact definitions of which have the meanings assigned to them by the GDPR:

- Right to information as to the personal data processing performed and the rationale of such processing
- Right to access to the personal data being processed for his / her person
- Right to rectification allowing individuals to request the correction or amendment of their data
- Right to object to a specific type of processing, under specific circumstances
- Right to object to automated processing or profiling in cases where automated processing results in decisions that in the opinion of the affected data subject, do not adequately reflect the unique characteristics of the case involved
- Right to withdraw consent allowing a data subject to give notice and withdraw a previously given consent for a specific type of processing
- Right to data portability allowing the transfer of personal data processed by a Data Controller to the data subject or directly to another Data Controller in electronic, machine readable format

- Right of Erasure ("right to be forgotten") entitling a data subject – under certain circumstances - to request the deletion of their personal data.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights as listed above). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. In extreme cases, we may even refuse to comply with your request in such circumstances.

K. Queries & Complaints

PHOENIXPRO is committed to acknowledge, consider and respond to all queries and complaints that it receives from any natural person who believes is affected by PHOENIXPRO's processing of his / her data. To communicate such queries or complaints please contact us on dpo@phoenixpro.com, and we shall seek to respond to the substance of your query as soon as practical, within a 30 day window as stipulated by GDPR.

If despite our responses and actions to address your concerns, you are not satisfied, you have the right to address the matter to the Data Protection Commissioner in your jurisdiction, details of which are listed below.

Country	Address	Telephone	eMail	Website
Cyprus	Jason street 1, 2nd Floor, Nicosia 1082	+357 22818456	commissioner@dataprotection.gov.cy	www.dataprotection.gov.cy
Greece	Kifissias 1-3, 115 23 Athens, Greece	+30 210 6475600	contact@dpa.gr	www.dpa.gr/
Bulgaria	2 Prof. Tsvetan Lazarov Blvd., Sofia 1592	+359 899 877 156	kzld@cpdp.bg	www.cpdp.bg/en/

L. Other Important Information

This Privacy Policy does not alter in any way other than explicitly defined herein, the obligations and responsibilities of PHOENIXPRO or its customers, employees, vendors or partners, all of which are governed by the respective contracts (where applicable) and related arrangements between PHOENIXPRO and each of those customers, employees, vendors or partners.

M. Use of Cookies

Cookies on Our Websites

PHOENIXPRO uses cookies on our websites. This is done to facilitate easier navigation throughout the website and increase visitor convenience. Your internet browser is likely to accept these cookies by default, however you can refer to your browser's help guide if you would like to reject or even delete them from your system.

According to www.allaboutcookies.org, Cookies [2] are small, often encrypted text files, located in browser directories. They are used by web developers to help users navigate websites efficiently and perform certain functions. Due to their core role of enhancing / enabling usability or site processes, disabling cookies may prevent users from using certain websites or specific areas or functionality of such websites.

Cookies are created when a user's browser loads a particular website. The website sends information to the

[2] Also known as browser cookies or tracking cookies

browser which then creates a text file. Every time the user goes back to the same website, the browser retrieves and sends this file to the website's server. Cookies are created not just by the website the user is browsing but also by other websites that run ads, widgets, or other elements on the page being loaded. These cookies regulate how the ads appear or how the widgets and other elements function on the page.

We may use both "session [3]" cookies and "persistent [4]" cookies on the website. We will use the session cookies to: keep track of you whilst you navigate the website; and other uses. We will use the persistent cookies to: enable our website to recognise you when you visit; and other uses.

Cookies used by PHOENIXPRO websites do not retrieve any personal information or any information from the visitor's computer.

To learn more about advertisers' use of cookies the following links may be helpful:

- European Interactive Digital Advertising Alliance (EU)
- Internet Advertising Bureau (EU)

Social Media Features and Widgets

Our Website includes Social Media features, such as the Facebook Like button and widgets, such as the Share this button or interactive mini-programs that run on our Website. These may collect your IP address, which page you are visiting on our Website, and may set a cookie to enable the Feature to function properly. Social Media features and widgets are either hosted by a third party or hosted directly on our Website. Your interactions with these features are governed by the privacy policy of the company providing it.

[3] Session cookies are typically deleted from your computer when you close your browser
[4] Persistent cookies remain stored on your computer until deleted, or until they reach a specified expiry date

N. Glossary & Useful Definitions

#	Term	Definition
1.	Personal Data	Also referred to as "personally identifiable information (or "PII"), personal data is any information relating to an identified or identifiable living natural person (the "data subject")
2.	Legal Basis of Processing	The basis on which the processing of personal data may be based and may be one of the following: • the consent of the data subject to the processing of his / her personal data • processing is necessary in order to enter into a contract to which the data subject is a contractual party or to take action at the request of the data subject before or after a contract is entered into force • processing is necessary to comply with a statutory obligation of the Data Controller or the Data Processor as the case may be • processing is necessary for the purposes of the legitimate interests pursued by the Data Controller, unless such interest overrides the interest or fundamental rights and freedoms of the data subject who require the protection of personal data, in particular if the subject of the data is a child • processing is necessary to safeguard the vital interest of the data subject or other natural person • processing is necessary for the performance of an obligation performed in the public interest or in the exercise of public authority assigned to the Company.
3.	Legitimate Interest	Our lawful interests in conducting and managing our business to enable us to give you the best services and / or products and secure and private by design experience. In choosing to perform personal data processing under the legal basis of legitimate interest, we seek to ensure that we consider and balance any potential impact on you (both positive and negative) and your rights before doing so. As a general principle, we do not use your personal information for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).
4.	Data Controller	The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of processing of personal data.
5.	Data Processor	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.
6.	Data Protection Officer	A Data Protection Officer (or "DPO") is a security leadership role required by the GDPR. The DPO is responsible for (a) overseeing data protection strategy and implementation within an organization; (b) ensuring compliance with GDPR requirements; (c) the provision of advice to the Data Controller or the Data Processor and their staff in relation to personal data processing; and (d) to cooperate with Data Protection Authorities and supervisory bodies in all privacy and data protection matters.
7.	Cross-border Data Transfers	Transfers of personal data outside the European Economic Area in physical and / or electronic form