

Data Protection Policy of ICAP S.A.

"ICAP S.A.", Kallithea, Eleftheriou Venizelou Ave. number 2, 17676, with VAT number 996952940 (Gen. Com. Reg. No. 147989301000)

1. Field of Scope

This privacy policy lays out the way ICAP S.A. (hereinafter referred to as "ICAP") collects, uses, processes, stores, manages, and protects the commercial and financial information regarding entities and individuals (hereinafter referred to as "Personal Data"), so as to meet the data protection standards of the company and comply with the applicable law.

This privacy policy shall apply to all information (i) to whom any third party may have access (hereinafter referred to as the "Client") during the use of the Services (ii) that relates to the products and services (hereinafter referred to as "Services") provided by ICAP (including but not limited to Business Reports, Credit Risk, Watch, Alert, Credit.Eye, Data.Prisma, Sector Studies, Marketing Lists, D&B products, Custom products (xml, metafile), Findbiz, Trade, Kompass products, provision of GDPR related consultation services, printed editions, leading editions, digital solutions (google ads, viber, facebook etc) (iii) pertaining to candidate employee data collected during the recruitment process iv) pertaining to individuals (journalists) obtained during the process of updating the Press Release Database v) pertaining to visitors and clients of ICAP's website <https://www.icap.gr/> (hereinafter referred to as the "Website"). With regards to the services offered through the online platforms ICAP B2B (www.icapb2b.gr), Findbiz (<https://www.findbiz.gr/>) & ICAP Data Prisma (www.icapdataprisma.com) (hereinafter referred to as the "Platforms") or the mobile application «ICAP OnTheGo» (hereinafter referred to as the "Application") you may review the pertinent privacy notices by visiting the relevant platforms. ICAP is bound to protect the privacy of Visitors/Clients, individuals and other data subjects and adhere to the Data Protection legislation currently in effect.

2. Categories & Types of Collected Data

Data Collected:

A. Sole Proprietorships' Commercial and Financial Data: trading name, communication data, history, premises, staff number, activity, imports & exports information, customers, suppliers, represented firms, other commercial relationships, cooperating banks, participations in other legal entities, net sales figures, balance sheet, P&L accounts, business plans, documents submitted to tax authorities (E3), contracts of lease, trial balance, management

B. Sole Proprietorships' Transaction Data: payment orders, seizures, real estate auctions, movable property auctions, bankruptcy petitions, bankruptcy judgments, conciliation procedure data, pre-bankruptcy events, overdue debts to the State and to the Single Social Security Entity

C. Sole Proprietorships' Trading Activity Data: identification data (i.e.: name, Tax Registration No., registered address, sector, date of establishment), days of credit, invoice No., invoice issuance date, invoice value, maturity date, payment date, payment bill No., payment value, qualitative data concerning the transaction behavior (e.g. arrangement, factoring)

D. Sole Proprietorships' Credit Performance Data: loan performance data, customer's internal statuses depending on Sole Proprietorships' credit behavior, fraud indications

E. Companies' Trading Activity Data: company's identification data (i.e.: name, Tax Registration No., registered address, sector, legal form, date of establishment), days of credit, invoice No., invoice issuance date, invoice value, maturity date, payment date, payment bill No., payment value, qualitative data concerning the transaction behavior (e.g. arrangement, factoring)

F. Companies' Financial Data: company separate & group consolidated financial statements and interim financial statements, comprising of: balance sheet, P&L accounts, cash flow, changes on equity, notes, independent auditors' report, BoD or administration report (exclusively for financial statements)

G. Companies' Transaction Data: payment orders, seizures, real estate auctions, movable

property auctions, bankruptcy petitions, bankruptcy judgments, uncovered cheques, protested bills, mortgages, conciliation procedure data, pre-bankruptcy events, overdue debts to the State and to the Single Social Security Entity

H. Companies' Commercial Data: corporate name, communication data, history, premises, staff number, activity, imports & exports information, clientele, suppliers, represented firms, other commercial relationships, cooperating banks, participations in other legal entities, net sales figures, shareholder/partner structure, administration structure, management, business plans, documents submitted to tax authorities (E3), contracts of lease, trial balance

I. Companies Credit Performance Data: loan performance data, customer's internal statuses depending on company's credit behavior, fraud indications

J. Individuals Personal & Identification Data: first name, last name, Tax Registration No., identification card No., passport No., father's name, mother's name, date of birth, gender, address

K. Individuals Transaction Data: payment orders, seizures, real estate auctions, movable property auctions, bankruptcy petitions, bankruptcy judgments, overdue debts to the State and to the Single Social Security Entity

L. Individuals Data Concerning Relationship with Legal Entities: shareholder/ partner relationship, administrative relationship, participation in Board of Directors, management relationship

M. Individuals Other Personal Information: father's name, mother's name, date of birth, gender, address, occupation, business information of individual's working place, nationality, marital status, protected members, children, income, income source, family income, personal income, card owner (indication), detrimental check flag, guarantor detrimental check flag

N. Individuals Credit Performance Data: loan performance data, customer's internal statuses depending on individual's' credit behavior, fraud indications

O. Suppliers/Vendors: financial and accounting data (invoicing upon agreement sign-off, name, surname, Tax Registration No., bank account, address)

P. Candidates: CV details: name/surname, postal address, contact details (including e-mail address, mobile phone number, academic qualifications, working experience, hobbies, interests, references)

Q. Journalists: name, surname, company (Media), position, e-mail (business & personal), address, phone number (Business & Personal), fax, gender

R. Companies (Mass Media) contact details: media, company, email (Business & Personal), address, phone number, fax, website

S. Business Contact Details of Individuals & Companies: name, surname, company (Media), position, address, phone number, fax, e-mail, gender

T. Companies' Contact Details: company, owner, e-mail, address, phone number, fax, website, Social Media profiles (public info or info from personal contacts)

U. Website Visitor/Client Data: internet protocol address (IP), browser type and the operating system

Declaration Regarding The Processing of Personal Data By ICAP (by its capacity as Data Controller and Processor - in accordance with the General Data Protection Regulation EU 679/2016)

Why will ICAP process my Personal Data (PD)?

ICAP provides products and services containing commercial and financial information about legal entities, sole proprietorships and individuals on the basis of the intended purpose, such as described in paragraph 6 hereof. Their contents vary depending on the type and purpose of the provided service of ICAP. The lawful basis of the data processing is ICAP's legitimate interest and in some instances the consent of the data subjects.

In addition ICAP may collect personal data of candidate employees who are interested in working with ICAP for the sole purpose of examining the possibility of a future collaboration - employment. The legal basis for the aforementioned data collection is the consent of the data subject who provides the necessary information.

Furthermore ICAP collects through public sources on the basis of legitimate interest and directly through the data subjects, information on journalists with the purpose of updating on a continuous basis the press release database.

Information automatically collected when visiting and interacting in the Website: We inform you that your personal data and information that are collected and processed when you manage your account in the Website, are appropriate to the purpose for which they are collected and are required for the processing of your inquiries, applications and the use of ICAP Services.

In particular, when visiting and interacting with the Website, certain information may be automatically collected, such as:

- your computer's Internet protocol address (IP)
- the type of browser and the operating system

More specifically ICAP's website employs the use of various types of cookies. For a full description on the types of cookies used and the data collected through them, you may read our [cookies policy](#).

Moreover, when visiting and interacting with the Application certain information may be automatically collected, such as:

- your computer's Internet protocol address (IP)
- the type of browser and the operating system

ICAP does not manage, collect or process geolocation data, which are collected and processed exclusively by the companies providing operating systems for each device you use (in case of use of iOS-Apple Inc or in case of android - Google Inc). ICAP does not have access to the positioning refresh rate of GPS.

3. Data Collection Points

- 1) General Commercial Registry (Γ.Ε.ΜΗ website) – A, B, F, G, H,J, L
- 2) Internet (corporate sites) – A, F, H, L
- 3) Athens Stock Exchange Website – H, J
- 4) Teiresias S.A – G
- 5) Sole Proprietorships – A, B, L,
- 6) Chambers of Commerce and Industry – A, H
- 7) Corporates - Members of ICAP Trade Exchange Program – C, E
- 8) Dun & Bradstreet – C, E
- 9) Candidate employees – P
- 10) Business Cards – Q, R
- 11)Sectorial, non ICAP editions /guides (adBook, Media Guide Magazines, Newspapers etc) – Q, R
- 12) Google research (websites) – Q, R
- 13) Mass Media campaigns – T, S
- 14) Social Media – J, T
- 15) ICAP's Clients (Banks in the context of Credit Risk Modeling Projects & Credit Rating activities and Other Corporates in the context of Analytics Services) – D, I, J, M, N
- 18) Court Data Collection Network – B, G, J, K,
- 19) Website – U
- 20) Corporates – F, G, H, L
- 21) Independent Authority for Public Revenue – B, G, K
- 22) External collaborators O

4. Recipients & Transfer of Data to Third Parties

ICAP reserves the right to disclose the data subject's personal data to any member of its affiliate/subsidiary companies (parent company and its subsidiaries) or other third parties to the extent it is reasonably necessary for the purposes determined in this notice and in particular:

- Data subject's data will be transferred to the departments of ICAP that are competent for the smooth and trouble-free operation of the Website services and functions
- Data subject's data may be transmitted and become accessible by legal entities with which, we have entered from time to time into contractual agreements for the purpose of fulfilling our company's legitimate interest for the provision of our Services within our contractual terms framework
- Data subject's may be disclosed to cloud hosting providers for the purpose of storing and safeguarding the data with the appropriate technical and security measures
- Data subject's data may be transmitted, become accessible and processed by subsidiaries of our group within the European union, which apply the appropriate technical, physical and administrative security measures for the protection of the data from loss, misuse, damage, alteration, unauthorised access and disclosure, as provided by article 32 of the GDPR 679/2016
- During all data transfers, we always take all appropriate measures so as to ensure that the transmitted data are the minimum required for the intended processing purpose and that the conditions for legitimate and lawful processing will always be met. ICAP's partners to whom the personal data may be transferred, have signed the necessary data processing agreements or have made specific guarantees around transfers of personal data by implementing in their agreements Standard Contractual Clauses (Model Clauses)
- ICAP servers are hosted at IBM's data centre (hosting provider) located in Athens. You may find more information on IBM's privacy notice in the following link:
https://www.ibm.com/privacy/details/us/en/#section_2

5. Personal Data Retention Period

The data retention period depends on the lawful basis of processing, as set out in detail below:

- In case the lawful basis for processing is the exercise of legitimate interest, the processing of personal data is carried out for as long as it is considered necessary for the achievement of the intended statutory purpose of ICAP described in paragraph 6 below, and until such time the limitation period of any related claims has expired.
- In case the personal data of the Client Information are provided under their own consent within the framework of their registration in the services of the Website, we shall retain their data until the granted consent by the data subject has been withdrawn. In case the consent is withdrawn for any valid reason, we shall retain them for as long as it is required until the limitation period of any related claims expires.
- In case the lawful basis for processing is the performance of the contract, we shall retain your data for as long as you retain the contractual relationship with ICAP in hard copy and in electronic form or we shall retain them for as long as it is required until the limitation period of any related claims expires.
- In case the lawful basis for processing is to take necessary steps at the request of the data subject prior to entering into a contract (such in the case with CVs of the candidate employees), we shall retain the pertinent personal data until the parties to agree to collaborate by signing an employer-employee agreement. On the event that no employment takes place, the data contained in the CV's are removed from ICAP's databases.

6. Legitimate Interest - Intended Purpose - Lawful Basis for Data Processing

ICAP operates as Credit Rating Agency since the 7th of July 2011, in accordance with the approval it received from the Hellenic Capital Market Commission and the European Securities & Markets Authority (ESMA).

ICAP within the framework of the general business activity according to the above and the pursuit of its statutory objectives, among which it is the collection, management, and provision of commercial and financial information (business information) regarding the transactors' evaluation of the creditworthiness and the promotion of its business activity for the assessment of the credit risks and the resolution of transactions, has created and maintains a database, which is daily updated with economic and commercial information in terms of economic units details. ICAP processes and stores the said data within the E.U.

Moreover, in cases where the Clients register and use the Website and Services of ICAP

(including those offered by www.icapb2b.gr or through the Application they will be requested to provide certain personal data. The data processing in this instance, is deemed necessary for the conclusion of a contract with ICAP, as well as for the use of the aforementioned applications, Services and Websites. Indicative personal data requested by the Clients in order to register and enable the use of the Services are the following: full name, company title, company vat number, registered address, corporate e-mail, country of registration.

7. Rights of the Data Subjects

You may exercise, as the case may be, the rights deriving from the applicable Greek Legislation and the General Data Protection Regulation (Regulation (EU) 2016/679) which are as follows: (a. the right of information (article 13), b. the right of access (article 15), c. the right to rectification (article 16), d. the right to erasure “right to be forgotten” (article 17), e. the right to restriction of processing (article 18), f. the right to data portability (to receive your personal data in a structured and commonly used format - article 20 where applicable) and g. the right to object (article 21) which applies to certain data processing activities

- These rights shall be exercised free of charge for you by sending a relevant letter to the Data Protection Officer (DPO) of ICAP: Eleftheriou Venizelou Street, number 2, Kallithea, PC 17676, Athens, ICAP S.A., +302107200000 or via e-mail to privacy@icap.gr. Alternatively, you may also visit our Subject Access Request page on our website [[SAR Form online](#)]. You can also submit your request in writing using the form in Appendix 1, sending the request to:
 - Complaints / Customer Care Department of ICAP: Eleftheriou Venizelou Street, number 2, Kallithea, PC 17676, Athens
 - Data Protection Officer (DPO) of ICAP: Eleftheriou Venizelou Street, number 2, Kallithea, PC 17676, Athens

- In case however the aforementioned rights are exercised excessively and without good cause thus causing us administrative burden, we may charge you with the cost related to the exercise of the respective right.
- In case you exercise any of your rights, we will take all appropriate measures available for the satisfaction of your request within thirty (30) days following the receipt of the relevant request. We may either inform you on the acceptance of your request or on any objective grounds that hinder the processing of your request.
- Notwithstanding the above, you may at any time object to the processing of your Personal Data, by withdrawing your consent (article 7, par. 3 of the GDPR 679/2016) by sending a letter to the Data Protection Officer (DPO) of ICAP: Eleftheriou Venizelou Street, number 2, Kallithea, PC 17676, Athens, or via e-mail to privacy@icap.gr. This right applies only in cases where the lawful basis for the data processing is the consent of the Data Subject.

8. Data Processing by ICAP

In some instances, our clients provide their business data, such as customer, supplier or third parties' data - which may contain personal data (who may refer to individuals or companies) - within the framework of provision of our services. In such cases, ICAP shall operate as the “Processor” of the personal data, which are included in the said business data. Consequently, in those cases different provisions of the GDPR 679/2016 shall apply, with which we comply. Additionally, ICAP applies throughout the data processing procedure, the appropriate technical, physical, and administrative security measures for the protection and security of the personal data from loss, misuse, damage or modification, unauthorised access and disclosure, in compliance with article 32 of the GDPR 679/2016, in order to ensure the appropriate security level against those risks. Those include, among others, as the case may be: **a)** application of encryption protocols **b)** the ability to ensure confidentiality (article 90 GDPR 679/2016), the integrity, availability, and resilience of processing systems and services on an ongoing basis, **c)** the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, **d)** a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. Moreover, ICAP shall take measures so as to ensure that any physical person acting under the authority of the data controller or of the processor, who has access to personal data, shall not process those data except on instructions from the data controller and limits access to your personal information to authorised employees.

Indicative security measures applied by ICAP are as follows:

- ICAP has been awarded with ISO 27001/2013 Certification
- ICAP maintains a dedicated information security team that plans, implements and provides surveillance of our information security program
- The company controls the security and functionality of its products and services before they are introduced to the Internet, for any vulnerabilities in technology
- The company performs ongoing infrastructure checks to detect weaknesses and potential intrusions, vulnerabilities in systems etc.
- The company uses **https** protocols for secure and encrypted client communication with ICAP
- The company uses the open standard protocol to access Lightweight Directory Access Protocol (**LDAP**) directory services and uses encrypted passwords
- The company uses a Secure Sockets Layer (SSL) certificate to create an encrypted connection between the web server and the Client's browser
- The company protects its Web Sites by presenting a Web Application Firewall and an IDS/IPS Firewall in-front of the Web Servers
- The company operates an ISMS - Information Security Management System to reduce Cyber-Security Risks.

9. Profiling

We use the information we obtain to produce scores and ratings such as ICAP's Failure and Delinquency Scores, ICAP's Maximum Credit etc. We may also carry out customized profiles for our customers. We use highly developed scoring models and algorithms, based on previous similar circumstances, adverse events and economic forecasts to produce a score. We recommend to our customers to interpret and use our scores by their own standards. Our customers may choose to use our scores individually or combine the scores with other information available to them. Their decision making will be based around whether to insure or market to, extend credit, acquire, trade or partner with a business entity. Our scores predict the probability of default and/or bankruptcy whether a business is likely to continue trading, pay its bills on time, receive credit, whether they would be likely to purchase a product or service, where they benchmark within their industry or whether they are subject to any specific risks. We do not make any decisions for an organization – nor do we maintain blacklists and we do not encourage our customers to decide whether to trade with an organization.

10. Submission of Complaint - Appeal

- For any issue regarding the processing of your personal data, you may contact us via e-mail at, customercare@icap.gr
- Moreover, you shall always be entitled to contact the Hellenic Data Protection Authority, which may accept the submission of relevant complaints in writing at its protocol in its offices at 1-3, Kifisias Street, Postal Code 115 23, Athens or by e-mail (contact@dpa.gr) in accordance with the instructions indicated on its website.
- If you no longer wish to receive newsletters from ICAP, please send an e-mail by visiting the link 'Newsletter' at ICAP Web Site or follow the unsubscribe instructions included in each relevant email/communication.

11. Amendments

This policy may be renewed from time to time, due to amendments to the related legislation or change to the corporate structure of ICAP. Thereby, we encourage the Clients to periodically visit this site so as to be informed regarding recent information of privacy practices. In any case, the Clients may be informed by e-mail or a notice in our Website regarding any amendments to this policy.