MCA People Solutions – Privacy Data Policy

Privacy Policy

It is the Policy of MCA People Solutions provide for the protection of privacy data as defined in Applicable Law(s). Protection of MCA People Solutions employee, customer, vendor and internet web browsers data (collectively all data subjects) is one of the most important principles for the conduct of business by MCA People Solutions. MCA People Solutions will act in a transparent and responsive manner to respond to the questions of data subjects, secure the privacy data and report to data subjects, minimize the privacy and confidential data we retain through our retentions and deletion standards and practices and report to government authorities and our customers identified by Applicable Law(s) in the event of a data breach. MCA People Solutions will manage our support services vendors to these same Applicable Law(s) and standards through our contractual documentation and when required, through audits.

Applicability, Purpose and Scope

With this privacy policy, MCA People Solutions (MCA) will provide for data subject Rights" as described in Applicable Law(s). MCA will inform inquirers about the type, scope and purpose of the personal data collected, used and processed by us and our vendors. Therefore, we inform you pf the following:

1. Contact information

MCA People Solutions will act according to the definitions of Applicable Law as either a data Controller or Processor. :

MCA PEOPLE SOLUTIONS
Argentine Street, Makassed Bldg,4th flr
2014-5002 Beirut central district, Lebanon
You can reach us via the contact form: hassan.chaker@mca-ps.com

Data Protection Officer:
Ms. Ghusam Ladki
MCA PEOPLE SOLUTIONS
Argentine Street, Makassed Bldg,4th flr
2014-5002 Beirut central district, Lebanon

If you want to assert your legal rights or have general questions, please contact ghusam@mca-ps.com or the corporate data protection officer of MCA People Solutions.

2. Data do we collect and process

a) Contract data
We collect, process and store the data you provide when you order from us. In addition, we store and process data about the order and payment history.

b) Data that you store on our servers
We collect, process and store the information you submit/store yourself when you use our services. This includes the production of backup copies in our backup systems. We store your data on our servers for a maximum of 15 days under the following circumstances.

c) Log data
When you visit our website or use our services, the device that you use to access the page

automatically transmits log data (connection data) to our servers. Log data includes the IP address of the device that you use to access the website or service, the type of browser you are using, the website you have visited beforehand, your system configuration, and the date and time. We store IP addresses only to the extent necessary to provide our services. Otherwise, the IP addresses are deleted or made anonymous. We store your IP address when visiting our website for a maximum of 7 days to detect and ward off attacks.

d) Customer correspondence
We process the data that is collected when you contact us by email, fax or post, for example.

e) Cookies, pixels, and other procedures
We use cookies, pixels, and similar technologies at several points on our web offerings.
Cookies are small bits of identification data that a server saves on a device that you use to access our website or our services. They contain information that can be read when accessing our services, thereby allowing for a more efficient and better utilization of our offerings.
We use both permanent and session cookies. Session cookies are deleted when your web browser is closed. Permanent cookies remain on your device until they are no longer necessary to achieve their purpose and are deleted. •For example, we use first-party cookies to record information about your user behavior on our website. •Third-party cookies do not come from MCA but from a third-party provider. We use these cookies, for example, for marketing activities.

Pixels are small graphics on websites which allow log files to be recorded and analyzed, which is often used for statistical evaluations.

A tag is an umbrella term for snippets of code which are integrated into websites and used for various functions, such as simple counters ("tracking pixels") or complex data transmissions (e.g "conversion tracking tags").

A script (also JavaScript) is able to execute more complex instructions, just like a programming language

We use the term "cookies" as a commonly used umbrella term. It also includes tags, pixels, and scripts as alternative technical implementations.

The procedures we utilize can be subdivided into various categories. Except for cookies which are technically necessary, you can decide which cookies you wish to permit.

You can change your settings later at the bottom of the page under "Cookie settings".

Some of the cookies process data in third countries. You can find out what these are in the respective cookie categories. When processing your data on the basis of these cookies, it is possible that the European level of data protection cannot be guaranteed. If you consent to processing using these cookies, you also consent to transferring and processing your data in these third countries in accordance with Article 49 (1) lit. a GDPR. For EU-UK General Data Protection Regulations (GDPR) compliance this may include additional contract requirements (EU Standard Contractual Clauses)

Necessary cookies

Statistics and analysis

f) Cookie setting via YouTube video embedding
We include videos from youtube.com on our website, especially on our Help & Contact page and our blog. We have embedded the videos in the so-called "extended privacy mode". This means that cookies are set by YouTube on the device you are using only after the play function is used, which can also serve to analyse usage behaviour for market research and marketing purposes.

If you have not agreed to cookies in the Partnership category, you must agree to the transfer of data to YouTube before playing a video. You can change your settings at any time at the bottom of the page under "cookie settings".

You can find out more about cookie usage by YouTube in Google's cookie policy at https://policies.google.com/technologies/types?hl=en-GB.

g) Newsletter tracking by Episerver:The operating company of the application is Episerver GmbH.The newsletters are provided by Episerver with a pixel-sized file that is retrieved from the server when the newsletter is opened. As part of this retrieval, information about the browser and your system, your IP address and whether and when the newsletters are opened are collected.

Links in the newsletters are individual, so that it can be tracked whether you have clicked on them.

In addition, a post-click tracking cookie is set. This makes it possible to track user actions even after leaving the newsletter. Among other things, purchases, registrations and downloads on the MCA website are recorded.

The analyses carried out by Episerver on the basis of the data collected are made available to us in summarized form in anonymized form, so that it is no longer possible to draw conclusions about the actions of individual recipients.

We use these statistical analyses to improve the accessibility of our offers and to ensure that you only receive content from us that corresponds to your interests. Our aim is also to optimize websites and to assess the success of advertising campaigns.

While the post-click tracking cookie is only set with your consent, the other tracking measures are carried out within the scope of our legitimate interests. You have the option to object to the collection and processing of data by Episerver in the customer login under the tab "Change customer data"-> "Contact ways".
h) Integration of Google services with MCA Webmail

MCA Webmail`s use and transfer to any other app of information received from Google APIs will adhere to Google API Services User Data Policy, including the Limited Use requirements.

3. Legal basis of the processing

We process and use your data to execute the contract and provide our services, to improve our services and our websites and to adapt them to your needs and to provide updates and upgrades.

Article 6 I lit. a of the General Data Protection Regulation (GDPR) provides us with a legal basis for processing operations, in which we obtain consent for a particular processing purpose. If the

processing of personal data is required to fulfil a contract, the processing is based on Article 6 I lit. b GDPR. The same applies to processing operations that are necessary to carry out pre-contractual measures, for example in cases of enquiries regarding our products or services. If we are subject to a legal obligation which requires the processing of personal data, such as the fulfilment of tax obligations, the processing is based on Article 6 I lit. c GDPR. Finally, processing operations could be based on Article 6 I lit. f GDPR. Processing operations that are not covered by any of the aforementioned legal bases are based on this legal basis if the processing is necessary for the protection of our legitimate interests or those of a third party, unless the interests, fundamental rights and fundamental freedoms of the person concerned (data subject) prevail. Such processing operations are particularly permitted because they have been specifically mentioned by the European legislator. A legitimate interest is usually to be assumed if the data subject is a customer of the controller.

If the processing of personal data is based on Article 6 I lit. f GDPR, our legitimate interest is conducting our business. This also includes data analysis to improve our products and services. As well as performance of legal obligations, insofar as processing does not fall under Article 6 (1) lit. c GDPR.

We process applicant data in accordance with Article 88 GDPR in conjunction with § 26 of the Federal Data Protection Act (BDSG, new version).

4. Categories of recipients

Registrars and registries: For domain registrations, we must forward certain personal data to registrars and registries. This data is stored in the registries' databases and publicly available to a varying extent via Who is enquiries from the registries. Further information about this can be found here https://www.MCA.com/faq/en_us/article/2098/What-is-WHOIS-and-which-data-is-stored-there.html

Escrow services: All registrars accredited by the Internet Corporation for Assigned Names and Numbers (ICANN) must, in accordance with ICANN's generic domain rules, hold the domain data they manage in a secure environment in trust. This is intended to ensure the reliable management of the namespace. To that end, we use the escrow services of DENIC eG, Kaiserstraße 75-77, 60329 Frankfurt am Main.

Collection service provider: These provide collection services for us.

Processors: We pass on various personal data to our processors as the controller within the scope of the processing. We have ensured the security of your data by concluding data processing protection agreements. Our processors can be divided into the following categories:

- Provision of services: These include newsletter delivery, printing and shipping of invoices, customer surveys, payment service providers, data carrier destruction
- Operation of services, maintenance and upkeep of hardware and software

We only release data to authorities and third parties in accordance with statutory provisions or a legal title. Information may be provided to authorities on the basis of a legal regulation on security or for prosecution purposes. Third parties will only receive information if required by law. This may be the case, for example, in the case of a copyright infringement.

5. Data transmission to sub-contractors and to third countries

Microsoft: To create your Microsoft Office 365 Business Account, we forward the following data to Microsoft Ireland Operations Ltd: Name, address, e-mail address and language. This data, as well as data that you store in Microsoft Office 365, can be processed in various Microsoft data centres around the world. The processing is carried out on the basis of the EU standard data protection clauses in accordance with Article 46 (2) lit. c GDPR.
Registries: For the registration of top-level domains. Processing is carried out on the basis of Article 49 (1) lit. b GDPR.
Dropsuite: In order to provide you with MCA mail archiving, we use software developed and operated by Dropsuite Ltd. In support cases, there is the possibility of remote access from Singapore. The archived contents themselves are stored on our servers in Germany. Processing is carried out on the basis of the EU standard data protection clauses pursuant to Article 46 (2) lit. c GDPR.

DigiCert: We act as intermediaries in the procurement and maintenance of SSL certificates. We transfer your data to Digicert Inc. in the USA so that Digicert can provide its service. Processing is carried out on the basis of Article 49 (1) lit. b GDPR.

Sitelock: When using SiteLock, LCC, malware in your webspace is automatically detected and deleted. We act as an intermediary and provide Sitelock with your domain names for this purpose. SiteLock saves your webspace for 7 days. Processing is carried out on the basis of Article 49 (1) lit. b GDPR.

Hewlett-Packard-Enterprise: For the maintenance and support of your servers, support access (remote access) can be provided by the Hewlett-Packard-Enterprise Company from the USA in individual cases of faults. For this purpose, an activation is made in individual cases, which is closed again after the end of the task. To ensure lawfulness, we have concluded EU standard data protection clauses in accordance with Article 46 (2) lit. c GDPR.

Salesforce: Our order processor for the MCA homepage design service, web4business, uses the CRM software Salesforce. In support cases, there is the possibility of remote access by Salesforce Inc. from the USA. Processing is carried out on the basis of the EU standard data protection clauses pursuant to Article 46 (2) lit. c GDPR.

IQ-to-Link: IQ-to-Link GmbH: provides us with call centre services from Kosovo via remote access, insofar as support requests require this. (To ensure lawfulness, we have concluded EU standard data protection clauses in accordance with Article 46 (2) lit. c GDPR.)

Genesys: when you contact us, your phone number and the area you are calling from are stored at AWS (Amazon Web Services) in Europe by Genesys Telecommunications Laboratories B.V.. This company operates our telephone system. In addition, your customer number, service pin and details of your products are also cached in AWS Europe. If you have given your consent to the recording of the call at the beginning of the call, this will also be stored. Both the storage and the transmission are exclusively encrypted. In individual support cases, there may be remote access to the data from the USA. However, these are only individual cases, which must be enabled by us in advance. To ensure legality, we have concluded EU standard data protection clauses in accordance with Art. 46 Para. 2 lit. c GDPR.

Selling Data

MCA does not sell privacy data nor client confidential data, and prohibits by contract language with and between its sub-contractor data processors from selling data provided by data controllers and other processors.

6. Duration Of Storage

We only process and store personal data for the period required to achieve the purpose of storage or where required by law. As a rule, the processing purpose is achieved upon termination of your contract.

You can change and delete data that you save in our services yourself. After the termination of contract, we will delete the data stored in the services.

Backup copies in our backup systems are automatically deleted with a time delay.

For contract data, processing will be restricted after the contract has been terminated; it will be deleted after expiry of the statutory retention period. We do not retain your data longer than seven years if necessary for financial audit compliance. Privacy and confidential data that MCA People controls on our servers will not be retained more than an agreed and lawfully justified period as agreed with out customers by contract.

7. Your Rights as protected in law

a) Right to information and confirmation
You have the right to receive free information from us at any time, as well as confirmation of your personal data stored and a copy of this information.

b) Right to rectification
You have the right to demand the immediate correction of incorrect personal data concerning you. You also have the right to request the completion of incomplete personal data, including by means of a supplementary statement, taking into account the purposes of processing.

c) Rights to erasure
You have the right to have your personal data erased without delay if any of the following is true and if processing is not required:

- The personal data has been collected for such purposes or processed in a way for which it is no longer necessary.
- You revoke your consent, on which the processing was based, and any other legal basis for processing is lacking.
- You object to the processing in accordance with Article 21 (1) GDPR and there are no legitimate reasons for the processing, or you object to the processing in accordance with Article 21 (2) GDPR.
- The personal data has been processed unlawfully.
- The erasure of personal data is required to fulfil a legal obligation under European Union law or a national law to which we are subject.
- The personal data was collected in relation to information society services offered pursuant to Article 8 (1) GDPR.

d) Right to restriction of processing
You have the right to request the restriction of processing if one of the following conditions is met:

- The accuracy of your personal information is contested by you for a period of time that allows us to verify the accuracy of your personal information.

- The processing is unlawful, you refuse the deletion of the personal data and instead require the restriction of the use of personal data.
- We no longer need your personal information for processing purposes, but you need it to assert, exercise or defend your rights.
- You have objected to the processing in accordance with Article 21 (1) GDPR and it is not yet clear whether our legitimate interests prevail over yours.

e) Rights to object
You have the right to object at any time to the processing of personal data concerning you, which takes place on the basis of Article 6 (1) lit. e or f GDPR.

In the event of an objection, we will no longer process personal data unless we can demonstrate compelling legitimate reasons for processing that outweigh your interests, rights and freedoms, or the processing serves the purpose of asserting, exercising or defending legal claims.

You have the right to object at any time to the processing of your personal data for the purpose of direct advertising.

f) Right to data portability
You have the right to receive personal data relating to you that has been provided to us in a structured, common and machine-readable format. You also have the right to transfer this data to another controller without hindrance by us if the processing is based on the consent pursuant to Article 6 (1) lit. a GDPR or Article 9 (2) lit. a GDPR or is based on a contract pursuant to Article 6 (1) lit. b GDPR and the processing is carried out by automated means, unless the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Furthermore, in exercising your right to data transferability under Article 20 (1) GDPR, you have the right to arrange that your personal data is transmitted directly from one controller to another, where this is technically feasible and as long as this does not affect the rights and freedoms of others.

g) Right to withdraw consent under data protection law
You have the right to withdraw the consent to the processing of personal data at any time.

h) Right of appeal to the supervisory authority
You have the right to contact a supervisory authority in the Member State of your place of residence or place of work or the location of the alleged violation at any time if you believe that the processing of personal data concerning you is contrary to the EU General Data Protection Regulation.

8. Data security

1.1. MCA shall encrypt all Data and any approved sub-processors process while the Data is in motion or at rest. Unless The client specifies a standard in the Agreement or a Statement of Work, MCA shall encrypt using a commercially acceptable, non-proprietary algorithm.
1.2. MCA will all not use pseudonymisation (replacing one attribute in a record by another) or de-identification (deleting some attributes, while other attributes are still identifiable) while processing any Data unless MCA has informed The client of its proposed approach before taking any such action and The client has approved such action.
1.3. If processing of Data occurs on a system owned, controlled, or operated at the authorization or direction of MCA or using software provided by or on behalf of MCA, then MCA shall ensure that MCA System and/or Software (excluding physical premises) processing the Data is securely configured,

including, but not limited to, disabling all unnecessary services or features and closing all known and all published security deficiencies therein, including updates and subsequently identified publications thereof after they are available to users.
MCA shall disclose all known deficiencies that cannot be mitigated to The client, to enable The client to perform a risk evaluation if necessary.
1.4. If processing of Data occurs on a MCA System or using MCA Software, or any agreed and approved third-party SaaS system or software in Annex A.2, then MCA shall apply all applicable security software patches/automatic system updates from the provider, for MCA System and/or Software as soon as possible after they become available to MCA.
In the event the patches are received as a patching emergency notice, then a prompt evaluation and installation response for patches rated critical and high by the vendor or through the CERT Vulnerability Notes Database, is expected, otherwise a commercially reasonable timeframe is agreed in the table below after they are available to users shall be required, unless a consultation with The client takes place after receipt of the patches and dictates a different decision.
MCA will not use end of life or unsupported software.

Patching Schedule for MCA and Sub Processors

Critical Rating Patch Installation	Not to Exceed 7 days from Notification
High Rating Patch Installation	Not to Exceed 45 days from Notification
Medium Rating Patch Installation	Not to Exceed 90 days from Notification
Low Rating Patch Installation	Not to Exceed 180 days from Notification

1.5. If processing, receiving and/or storing of Data occurs on a Supplier System, then MCA shall continuously maintain industry-standard firewall protection for Supplier System.

1.6. MCA provides servers storing Data and the servers accept connections, MCA will only accept authenticated connections that are necessary for proper operation of MCA System and/or Software in conformity with the Agreement.
1.7. If processing of Data occurs on a MCA System, standard machine settings to maintain access logs must be enabled. MCA will not tamper access logs.
1.8. If processing of Data occurs on MCA System or using MCA Software, or on a System owned, controlled, or operated at the authorization or direction of MCA, industry standard settings must be enabled to maintain access logs.
1.9. MCA shall make commercially reasonable efforts to ensure that any System components are free of Contaminants. Such efforts shall include, but are not limited to, running on a scheduled manual or automated process anti-virus software on all MCA Systems, updating signatures, conducting Contaminant sweeps of Systems and purging all Contaminants found.
MCA shall use commercially reasonable efforts to not transmit or distribute Contaminants. Any such transmission or distribution of Contaminants on a system or software used to interact with The client, its clients, or processors, is deemed to be a Security Incident and MCA, for itself and for its sub processors, must notify The client.
1.10. Although MCA is not ISO certified, MCA adheres to ISO/IEC 27001 security standards.

9. Statutory or contractual requirement, for the provision of personal data, necessity for the conclusion of the contract, obligation to provide the personal data, possible consequences of failure to provide data

The provision of personal data may in part be required by law (e.g. tax regulations) or result from contractual provisions (e.g. information about the contracting party). Sometimes it may be necessary that you provide us with personal data, which must subsequently be processed by us, in order to conclude a contract. For example, you are required to provide us with personal information when we conclude a contract with you. Failure to provide the personal data would mean that the contract could not be executed or concluded.