Privacy Policy
§ 1. General provisions

1. The Joint Controllers of the personal data of all clients of the MTA Group companies are:
   a. **MTA Digital sp. z o.o.** with its registered office in Poznań, at ul. Święty Marcin 29/8, 61-806 Poznań, entered in the Register of Entrepreneurs maintained by the District Court Poznań – Nowe Miasto i Wilda in Poznań, 8th Commercial Division, under KRS number: 0000561985, NIP: 7831727441, REGON: 36172305500000, with share capital of PLN 5,000.00, fully paid up, represented by Jakub Krystkowiak – President of the Management Board,
   b. **MTA Performance sp. z o.o.** with its registered office in Poznań, at ul. Święty Marcin 29/8, 61-806 Poznań, entered in the Register of Entrepreneurs maintained by the District Court for the Capital City of Warsaw in Warsaw, 12th Commercial Division, under KRS number: 0000784788, NIP: 7010922437, REGON: 383274210, with share capital of PLN 5,000.00, fully paid up, represented by Mateusz Mikołajczyk – President of the Management Board,
   c. **Anchor.Team sp. z o.o.** with its registered office in Poznań, at ul. Święty Marcin 29/8, 61-806 Poznań, entered in the Register of Entrepreneurs maintained by the District Court Poznań – Nowe Miasto i Wilda in Poznań, 8th Commercial Division, under KRS number: 0000969275, NIP: 7831856345, REGON: 521897892, with share capital of PLN 5,000.00, fully paid up, represented by Wiktor Jacheć – President of the Management Board,
   d. **Force of Nature Europe sp. z o.o.** with its registered office in Poznań, at ul. Święty Marcin 29/8, 61-806 Poznań, entered in the Register of Entrepreneurs maintained by the District Court Poznań – Nowe Miasto i Wilda in Poznań, 8th Commercial Division, under KRS number: 0001050399, NIP: 7831885358, REGON: 525999520, with share capital of PLN 5,000.00, fully paid up, represented by Jacek Matuszewski – Member of the Management Board,
   e. **Zero Fluff Digital sp. z o.o.** with its registered office in Poznań, at ul. Święty Marcin 29/8, 61-806 Poznań, entered in the Register of Entrepreneurs maintained by the District Court Poznań – Nowe Miasto i Wilda in Poznań, 8th Commercial Division of the National Court Register, under KRS number: 0001174081, NIP: 7831930082, REGON: 541841870, with share capital of PLN 5,000.00 fully paid up, represented by Jacek Matuszewski – Member of the Management Board,
   f. **SharkPress Agency sp. z o.o**. with its registered office in Poznań, at ul. Święty Marcin 29/8, 61-806 Poznań, entered in the Register of Entrepreneurs maintained by the District Court Poznań – Nowe Miasto i Wilda in Poznań, 8th Commercial Division of the National Court Register, under KRS number: 0001181847, NIP: 7831932253, REGON: 542142080, with share capital of PLN 5,000.00 fully paid up, represented by Wiktor Jacheć – President of the Management Board,
   hereinafter jointly referred to as the „**Joint Controllers of personal data**”:
2. The Joint Controllers have appointed a contact person for personal data protection matters, namely Mateusz Mikołajczyk, who can be contacted:
   a. e-mail: gdpr@mta.digital, or
   b. by writing to the correspondence address: Mateusz Mikołajczyk, ul. Święty Marcin 29/8, 61-806 Poznań,
   c. in person at the operational office of MTA Digital sp. z o.o. at ul. Bolesława Prusa 6/3, 60-819 Poznań (an office address, different from the registered seat).

§ 1a. The essence of the arrangements between the Joint Controllers (Article 26 GDPR)

The six Joint Controllers indicated in § 1 have entered into arrangements defining the scope of their responsibility for fulfilling the obligations arising under the GDPR, in particular as regards the performance of the information obligation and the handling of data subjects' requests (Article 26(1) GDPR). The common point of contact in all matters concerning personal data protection is the contact person indicated in § 1 (e-mail address: gdpr@mta.digital). The operational coordination of handling data subjects' requests and performing the information obligation is carried out by MTA Digital sp. z o.o.; this does not, however, establish any hierarchy between the Joint Controllers — they remain controllers on equal terms.

Regardless of the internal division of tasks, you may exercise the rights available to you against each of the Joint Controllers; none of them may refuse to handle a request on the grounds that another entity is operationally dealing with the matter (Article 26(3) GDPR).

The Joint Controllers are jointly and severally liable to you for damage caused by the joint processing of data, in order to ensure effective compensation (Article 82(4) GDPR).

The essential content of the arrangements between the Joint Controllers is made available to data subjects upon a justified request sent to gdpr@mta.digital.

§ 2. Grounds for processing, purposes, source and retention of personal data

We obtain personal data directly from you – you provide it to us e.g. when concluding contracts, in the course of performing contracts for you, and when making contact via the contact form. In order to provide you with the clearest possible information, we have grouped it by reference to the purpose of processing your personal data.

As part of providing Lead Generation services to our Clients, we also process the personal data of third parties („leads") obtained indirectly, i.e. not directly from the data subject, but from publicly available business databases and tools used to acquire contacts (e.g. Apollo.io, Instantly.ai, Mailforge, Findymail, Clay, Aimfox). The legal basis for processing this data is Article 6(1)(f) GDPR, i.e. the legitimate interest of the Joint Controllers and their Client consisting in conducting direct marketing (B2B). The scope of the processed data usually includes the first name, surname, position, company name, e-mail address and business telephone number.
Providing personal data is voluntary, but in many cases necessary to achieve the purposes indicated in the table below — in particular to conclude and perform a contract, to respond to an enquiry sent via the contact form, or to send the newsletter. Failure to provide personal data may result in the inability to conclude or perform a contract, respond to an enquiry, or achieve the other indicated purposes.

Purpose of processing personal data	Legal basis for processing personal data	Retention period of personal data	Scope of processed personal data
Conclusion and performance of a contract for the provision of marketing/promotional/search engine optimisation (SEO)/Lead Generation services/website development	Processing your personal data is necessary to perform the contract for the provision of services to you. The legal basis for processing personal data is Article 6(1)(b) GDPR, i.e. processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.	We will process your personal data for the duration of the provision of services to you. We will process the data at the latest until the expiry of claims under the concluded service contract.	E-mail address, first name, surname, street, house or flat number, country, telephone, bank account number, transaction amount, bank name. Where the Client is an entrepreneur, the following data is processed: company name, NIP, street, house or flat number, country, telephone. Where the first name and surname of the person placing the order on behalf of the Business Partner are provided, this data is also processed.
Conducting day-to-day business activity, including cooperation with business partners who supply the Joint Controllers with products and services necessary for a given Joint Controller's day-to-day activity	The legal basis for processing personal data is Article 6(1)(b) GDPR, i.e. processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.	Personal data will be processed for the period of the business cooperation or, as the case may be, until the expiry of all claims arising therefrom	first name and surname, company name, NIP, address, telephone number, e-mail address,
Contact with Clients via the contact form available at https://mta.digital/pl/kontakt/ and https://www.anchor.team/contact,	Processing your personal data is necessary in order to answer the question you asked via the contact form. The legal basis for processing personal	We will process your personal data for the time necessary to answer the enquiry and conduct the correspondence, and subsequently until the limitation of any claims	First name, surname, e-mail address,

	data is Article 6(1)(f) GDPR, i.e. the legitimate interest of the Joint Controllers consisting in responding to persons who contact the Joint Controllers. Where the enquiry is aimed at concluding a contract, the basis for processing is Article 6(1)(b) GDPR, i.e. taking steps at the request of the data subject prior to entering into a contract.	or until an effective objection to the processing is lodged.	
Statistics on the use of particular functionalities of the website https://mta.digital/pl/, https://www.anchor.team/pl and those of the other Joint Controllers.	Our legitimate interest consisting in facilitating the use of services provided electronically and in improving the functionality of those services. The legal basis for processing personal data in such a case is Article 6(1)(f) GDPR, i.e. the legitimate interest of the Joint Controllers.	We will process your personal data for the period during which cookies are stored, but no longer than for a period of 50 months	For these purposes, we process personal data concerning your activity, such as: data on how individual users use the Joint Controllers' website and their preferences in this respect, the amount of time spent on the website belonging to the Joint Controllers; the number of visits to specific URLs (subpages) from specific phrases or media channels, data on the location of the devices by means of which users display the websites belonging to the Joint Controllers, age, gender, other data on users' activity on the websites belonging to the Joint Controllers and on websites associated with them, e.g. on posted comments and reviews, activity on social networks, e-mail address, IP address, other online identifiers of users, e.g. login,
Establishment, pursuit and enforcement of claims. Own accounting	Our legitimate interest consisting in the establishment, pursuit and enforcement of claims, and in	The data is processed for the limitation period of claims resulting from the provisions of the Civil Code. All data processed for	For this purpose, we may process certain personal data provided by you: first name, surname, company name, residential address, NIP, REGON, PESEL, data

	defence against claims in proceedings before courts and other state authorities. The legal basis for processing personal data in such a case is Article 6(1)(f) GDPR, i.e. the legitimate interest of the Joint Controllers. In addition, we process data on the basis of Article 6(1)(c) GDPR in conjunction with Article 74(2) of the Accounting Act in conjunction with Article 86 § 1 of the Tax Ordinance (i.e. due to the need to fulfil obligations arising from legal provisions, e.g. accounting, bookkeeping and tax obligations).	accounting purposes and for tax reasons is processed for a period of 5 years, counting from the beginning of the year following the financial year in which the operations, transactions and proceedings were definitively concluded, paid, settled or time-barred (i.e. in accordance with Article 74(2) of the Act of 29 September 1994 on Accounting (consolidated text: Journal of Laws of 2023, item 120, as amended) in conjunction with Article 86 § 1 of the Act of 29 August 1997 – Tax Ordinance (consolidated text: Journal of Laws of 2025, item 111, as amended).	of an accounting, bookkeeping or financial nature, or data relating to the claim pursued (data concerning the use of our services, if the claims arise from the manner in which you use our services, and other data necessary to prove the existence of a claim, including the extent of the damage suffered).
Handling of online payments (payment gateway)	Processing your personal data is necessary to handle payments for the services provided by the Joint Controllers. The legal basis for processing is Article 6(1)(b) GDPR, i.e. processing necessary for the performance of a contract. As regards issuing and storing invoices and settlement documentation, the basis is Article 6(1)(c) GDPR in conjunction with accounting and tax law provisions. Furthermore, for the purpose of fraud prevention and transaction	We process data related to payment execution until the performance of the contract and the expiry of any claims arising therefrom. Data processed for accounting purposes and for tax reasons (including invoices) is processed for a period of 5 years, counting from the beginning of the year following the financial year in which the transaction was definitively settled.	First name, surname, e-mail address, billing address, payment instrument data (tokenised on the side of the payment gateway provider – the Joint Controllers do not store full payment card data), tax identifiers (NIP/VAT) and transaction data.

	verification and security, the basis is Article 6(1)(f) GDPR, i.e. the legitimate interest of the Joint Controllers. Payments are handled via an external payment gateway (currently Stripe) acting as a processor.		
Sending the newsletter	The legal basis for processing personal data for the purpose of sending the newsletter is the consent of the person to whom the newsletter is to be sent, expressed e.g. by ticking a checkbox. The legal basis for processing personal data in such a case is Article 6(1)(a) GDPR, i.e. the consent of the data subject.	Personal data processed for the purpose of sending the newsletter is stored until consent is withdrawn by the data subject. Withdrawal of consent does not affect the lawfulness of the processing of personal data carried out before its withdrawal.	For the purpose of sending the newsletter, we may process certain personal data provided by you: first name, surname, e-mail address.
Running social media profiles, including Facebook, Instagram, LinkedIn	The legal basis for processing personal data is Article 6(1)(f) GDPR, i.e. the legitimate interest of the Joint Controllers consisting in promoting the services offered by the Joint Controllers and in undertaking other marketing activities.	Personal data is processed for the period during which the natural person uses the pages made available by the Joint Controller via Facebook, Instagram and other social media.	The Joint Controllers process personal data made available by the natural person on social media, most often including: first name, surname, nickname, image, etc.
Bookkeeping, accounting	The legal basis for processing personal data is: Article 6(1)(c) GDPR in conjunction with Article 74(2) of the Accounting Act in conjunction with Article 86 § 1 of the Act of 29 August 1997 – Tax Ordinance, i.e. the necessity to fulfil a	The data is processed for the limitation period of claims resulting from the provisions of the Civil Code. All data processed for accounting purposes and for tax reasons is processed for a period of 5 years, counting from the beginning of the year following the financial year in which	Personal data such as first name, surname, company name, NIP, address, place of business, delivery address, bank account number.

	legal obligation incumbent on the Joint Controllers of Personal Data	the operations, transactions and proceedings were definitively concluded, paid, settled or time-barred (i.e. in accordance with Article 74(2) of the Act of 29 September 1994 on Accounting (consolidated text: Journal of Laws of 2023, item 120, as amended) in conjunction with Article 86 § 1 of the Act of 29 August 1997 – Tax Ordinance (consolidated text: Journal of Laws of 2025, item 111, as amended).	
IT support	The legalising premise is Article 6(1)(f) GDPR, the legitimate interest of the Joint Controllers consisting in ensuring the proper IT support of the services provided by the Joint Controllers. In addition, the Joint Controllers process personal data for IT support purposes in connection with the recruitment of Associates and employment, as well as in connection with conducting business cooperation with Business Partners.	Personal data is processed for the period during which cookies are stored. The Joint Controllers may process personal data for longer if this results from the primary purpose of processing the data (e.g. the Joint Controller processes personal data at the latest until the expiry of claims under the concluded contract).	Data resulting from cookies, as well as all other data that the Joint Controllers process in connection with IT support (e.g. data processed using electronic mail), including in particular the data of Clients, Business Partners and Job Candidates.
Operation of the partner programme	The legalising premise is Article 6(1)(b) GDPR, i.e. the necessity to process personal data in order to enable participation in the operation of the partner programme, as well as Article 6(1)(f)	Personal data is processed for the period of the business cooperation or until the expiry of any claims.	Data necessary to participate in the partner programme resulting from the form available at https://mta.digital/pl/program-partnerski-kontakt/ such as: e-mail address, company URL, interests, and the data necessary to conclude the Contract such as first name, surname, registered office

	GDPR, i.e. the legitimate interest of the Joint Controllers consisting in increasing the number of Clients using their services.		address, telephone number, company name, NIP, data of the person representing the given entity.
Running a blog on the website at: https://mta.digital/pl/blog-2/ and at https://www.anchor.team/blog	Legalising premise: Article 6(1)(f) GDPR, i.e. the legitimate interest of the Joint Controllers consisting in promoting their own services.	Personal data will be processed for the period during which the legitimate interest of the Joint Controllers of personal data exists, or until an objection is lodged.	Within the blog run by the Joint Controllers of Personal Data, data such as the following may potentially be processed: first name, surname, image.
Collecting Client reviews on the website at https://www.anchor.team/#Testimonials	Legalising premise: Article 6(1)(f) GDPR, i.e. the legitimate interest of the Joint Controllers consisting in surveying Clients' satisfaction with the quality of the services provided.	Personal data will be processed for the period during which the legitimate interest of the Joint Controllers of personal data exists, or until an objection is lodged.	As part of the activity of surveying Clients' satisfaction with the quality of the services provided, the following personal data is processed: first name, surname, company name.
Holding online conferences with potential clients	Legalising premise: Article 6(1)(b) GDPR, i.e. the necessity to process personal data prior to entering into a contract, and Article 6(1)(f) GDPR, i.e. the legitimate interest of the Joint Controllers consisting in enabling contact with Clients as quickly as possible.	Personal data will be processed for the period of the business cooperation or until the expiry of any claims.	As part of the personal data processing activity related to holding online conferences, the following personal data will be processed: first name, surname, e-mail address, and other data required by the Calendly application used by the Joint Controllers of Personal Data.
Recording, automatic transcription of online meetings and their subsequent processing	Article 6(1)(a) GDPR, i.e. the explicit consent of the data subject (expressed before the transcription/recording begins), and Article 6(1)(f) GDPR, i.e. the legitimate interest of the Joint Controllers consisting in optimising internal processes and managing	Until consent is withdrawn or an effective objection is lodged, but no longer than until the business notes are anonymised or the business purpose ceases.	Voice, image, first name and surname, e-mail address, position, and any other personal data voluntarily provided by participants during the recorded meeting.

	knowledge from projects.		
Running a form enabling the resolution of problems encountered by Clients in the course of business activity, via the website at https://www.anchor.team/contact	Legalising premise: Article 6(1)(f) GDPR, i.e. the legitimate interest of the Joint Controllers consisting in resolving Clients' problems related to their business activity, and Article 6(1)(b) GDPR, i.e. the necessity to process personal data in order to take steps prior to entering into a Contract	Personal data will be processed for the period of the business cooperation or until the expiry of any claims.	As part of the personal data processing activity related to running a form used to resolve problems encountered by Clients in the course of business activity, the following personal data will be processed: first name, surname, e-mail address, telephone number, website address (if it contains personal data).

§ 3. Recipients of personal data

1. The Joint Controllers of Personal Data transfer personal data only to the extent necessary to achieve the processing purposes specified in this Privacy Policy, on an appropriate legal basis and in compliance with the requirements concerning personal data protection.
2. Depending on the purpose of processing, the type of service provided and the functionalities used, the recipients of personal data may be:
    a. **providers of IT infrastructure, hosting, cloud services, databases and solutions ensuring the security and availability of services**, in particular the providers of Google, Home.pl, CyberFolks, lh.pl, mydevil.net, OVH, mikrus, Cloudflare, Supabase, Vercel, Netlify and Alibaba Cloud services,
    b. **providers of tools for creating, maintaining and operating websites, online stores and applications**, in particular the providers of Web Innovative Software, Webflow, Shopify, Bubble, ManageWP, Plesk, ploi.io, ACF Pro and WPML services — to the extent that the use of these services involves the transfer of personal data to their providers,
    c. **providers of systems for managing customer relationships, projects, tasks and documents, and for concluding and signing contracts**, in particular the providers of HubSpot, Pipedrive, ClickUp, Airtable, Atlassian, Notion, Autenti and Google Workspace services
    d. **providers of communication services and tools for organising, recording and processing meetings**, in particular the providers of Google Workspace, Slack, Zoom, Loom, Riverside, Twilio and Ringostat services
    e. **providers of tools for system integration, process automation and the transfer of data between services,** in particular the providers of Zapier, Make, trigger.dev, Airbyte services, and services used within the n8n, Embedchain and Pulse System – Google Apps solutions. For solutions maintained on own or rented infrastructure, the recipients may be the providers of that infrastructure and of external services connected to the given solution,
    f. **providers of tools supporting marketing, the acquisition and handling of business contacts, and electronic communication**, in particular the providers of Apollo, Instantly, Mailforge, Findymail, Clay, Aimfox, Resend, HubSpot, Intch, Linkhouse, Whitepress and PRNews services
    g. **providers of analytics, advertising, SEO and consent management tools**, in particular the providers of Google Analytics, Google Ads, Google Tag Manager, Microsoft Clarity, Meta Pixel, LinkedIn Insight Tag, TikTok Pixel, X Ads, Ahrefs, Similarweb, DataSlayer, Nightwatch, Screaming Frog, SEO BOT AI, Stape and Cookiebot services — to the extent that the functionalities used involve the processing of personal data,
    h. **providers of tools for creating and editing content and graphic, audio and audiovisual materials,** in particular the providers of Adobe, Canva, Figma, Filmora, ElevenLabs, Higgsfield, Magnific/Freepik, Confect, Adnova, CreativeOS, Creativeflow, arcads.ai, iStock, Streamline and Tinify services — if the use of these services involves the transfer of materials containing personal data,
    i. **providers of tools based on artificial intelligence and of services enabling access to AI models,** in particular the providers of ChatGPT, Claude/Anthropic, OpenRouter, Lovable, Cursor, Windsurf, Browser Use and Z.ai services. If a service acts as an intermediary in accessing other providers' models, the recipients may also be the providers of the models used to perform the given task,

j. **providers of other tools supporting the provision of services, content processing and process handling,** including the tools indicated as Feedr, Nanonoble, Fal Features Labels and Forge — if their use involves the transfer of personal data,
k. **providers of solutions for access management and information security,** in particular the provider of the LastPass service,
l. **banks, payment operators and payment gateway providers, in particular the provider of the Stripe service and other operators used to handle payments** — to the extent necessary to execute and settle transactions,
m. **postal operators, courier companies and intermediaries organising shipments**, in particular the provider of the Furgonetka service — to the extent necessary to carry out delivery,
n. **entities providing accounting, legal, advisory, audit and debt collection services**, including MSRR Szymańska sp. z o.o. sp.k.,
o. independent subcontractors, including those cooperating on the basis of B2B contracts, and other entities participating in the provision of services to Users and clients.

3. The data of a specific individual is not transferred to all the listed providers, but only to the recipients participating in the given processing process. The mere use of software, a library or a tool running on the Joint Controllers' infrastructure does not mean that data is transferred to its manufacturer.
4. Recipients may process data as processors acting on behalf of the Joint Controllers or as separate controllers, depending on the nature of the service provided and the applicable law. Where processing is entrusted, the Joint Controllers use entities providing sufficient guarantees to implement appropriate technical and organisational measures, and conclude agreements meeting the requirements of Article 28 GDPR.
5. Personal data may also be transferred to courts, law enforcement authorities, supervisory authorities and other authorised entities, if the obligation to transfer it arises from legal provisions. Data may also be transferred to entities participating in the establishment, pursuit or defence of claims, if there is an appropriate legal basis for such transfer.
6. The use of analytics, advertising and marketing tools takes place on the legal bases specified in this Privacy Policy. If the use of a given tool, or the storage of information on the User's device or access to such information, requires consent, these activities take place after it has been obtained.

§ 4. Transfer of data outside the EEA, including outside the European Union

1. In connection with the use of external providers' services, personal data may be transferred outside the European Economic Area (EEA), including outside the European Union. The EEA comprises the member states of the European Union and Iceland, Liechtenstein and Norway. Transferring data to these three countries does not constitute a transfer outside the EEA
2. Transfers of data outside the EEA may occur in particular in connection with the use of the following tools and services:
    a. as regards the provision of services related to the maintenance of infrastructure, websites and work systems

Tool	Provider / entity indicated in the documentation	Country of transfer	Mechanism for legalising the transfer of personal data
Google Workspace, Google Analytics, Google Ads, Google Tag Manager	Google Ireland Limited / Google LLC. – (for cloud services, the relevant entity depends on the contract)	USA	EU–US Data Privacy Framework (DPF) — the transfer to Google LLC is covered by DPF certification, on the basis of Article 45(1) GDPR and European Commission Implementing Decision (EU) 2023/1795 of 10 July 2023. For transfers not covered by the DPF — Standard Contractual Clauses (SCC) adopted by European Commission Implementing Decision (EU) 2021/914, on the

			basis of Article 46(2)(c) GDPR, in accordance with the terms of the relevant Google service
Alibaba Cloud	Alibaba Cloud (Singapore) Private Limited	Singapore	Standard Contractual Clauses (SCC) adopted by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, on the basis of Article 46(2)(c) GDPR, together with a transfer impact assessment (TIA) and, where necessary, additional safeguards.
Cloudflare	Cloudflare, Inc.	USA	EU–US Data Privacy Framework (DPF) – Article 45(1) GDPR, in connection with Commission Implementing Decision (EU) 2023/1795 of 10 July 2023, to the extent covered by the recipient's valid certification. If the DPF does not apply – Standard Contractual Clauses (SCC) in accordance with Article 46(2)(c) GDPR and Commission Decision (EU) 2021/914, included in the Cloudflare data processing agreement (DPA), together with a transfer impact assessment (TIA) and any supplementary measures.
Supabase	Supabase Pte. Ltd.	Singapore	Standard Contractual Clauses (SCC) adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 – Article 46(2)(c) GDPR, incorporated into the Supabase DPA: Module 2 for the controller–processor relationship or Module 3 for the processor–sub-processor relationship
Vercel	Vercel Inc.	USA	EU–US Data Privacy Framework (DPF) – Article 45(1) GDPR and

			Commission Implementing Decision (EU) 2023/1795 of 10 July 2023, to the extent covered by Vercel's valid certification. In addition, the provider's DPA provides for Standard Contractual Clauses (SCC) adopted by Commission Decision (EU) 2021/914 – Article 46(2)(c) GDPR, for transfers requiring this safeguard.
Netlify	Netlify, Inc.	USA	EU–US Data Privacy Framework (DPF) – Article 45(1) GDPR and Commission Implementing Decision (EU) 2023/1795 of 10 July 2023, to the extent covered by Netlify's valid certification. Alternatively: Standard Contractual Clauses (SCC) – Article 46(2)(c) GDPR and Commission Decision (EU) 2021/914 of 4 June 2021, in accordance with the provider's DPA.
Webflow	Webflow, Inc.	USA	EU–US Data Privacy Framework (DPF) – Article 45(1) GDPR and Commission Implementing Decision (EU) 2023/1795, provided that the recipient holds active certification covering the transferred data. Where the DPF does not apply: Standard Contractual Clauses (SCC) included in the Webflow DPA – Article 46(2)(c) GDPR and Commission Implementing Decision (EU) 2021/914.
Bubble	Bubble Group, Inc.	USA	Standard Contractual Clauses (SCC) included in the Bubble DPA – Article 46(2)(c) GDPR and Commission Implementing Decision (EU) 2021/914; Module 2

			(controller–processor) or Module 3 (processor–processor), depending on the client's role. If Bubble holds active EU–US DPF certification covering the given transfer, the DPF takes precedence – Article 45(1) GDPR and Commission Implementing Decision (EU) 2023/1795.
Shopify	Shopify International Limited for clients in the EMEA region, parent company Shopify Inc.	Canada	European Commission adequacy decision – Article 45(1) GDPR in connection with Commission Decision 2002/2/EC of 20 December 2001, concerning Canadian organisations subject to the PIPEDA Act.
ManageWP	GoDaddy.com, LLC	USA	EU–US Data Privacy Framework (DPF) – Article 45(1) GDPR and Commission Implementing Decision (EU) 2023/1795, to the extent covered by active certification. Where the DPF does not apply: Standard Contractual Clauses (SCC) included in the DPA – Article 46(2)(c) GDPR and Commission Implementing Decision (EU) 2021/914.
HubSpot	HubSpot, Inc.	USA	EU–US Data Privacy Framework (DPF) – Article 45(1) GDPR and Commission Implementing Decision (EU) 2023/1795, to the extent covered by active certification. In addition, Standard Contractual Clauses (SCC) incorporated into the HubSpot DPA – Article 46(2)(c) GDPR and Commission Implementing Decision (EU) 2021/914.
Airtable	Formagrid, Inc., operating as Airtable	USA	Standard Contractual Clauses (SCC) included

			in the Airtable DPA – Article 46(2)(c) GDPR and Commission Implementing Decision (EU) 2021/914 of 4 June 2021. Module 2 – controller–processor; Module 3 – processor–sub-processor , depending on the client's role.
Atlassian, e.g. Jira and Confluence	Atlassian Pty Ltd — the entity indicated in the current product terms; the group also includes Atlassian US, Inc.	Australia / USA	Australia – Standard Contractual Clauses (SCC) included in the Atlassian data processing agreement (DPA), adopted by Commission Implementing Decision (EU) 2021/914 — basis: Article 46(2)(c) GDPR. Atlassian indicates the SCC as the mechanism for direct transfers to Australia. USA – EU–US Data Privacy Framework (DPF) — for transfers to Atlassian US, Inc. and US affiliates covered by active certification, on the basis of Article 45(1) GDPR and Commission Implementing Decision (EU) 2023/1795. In cases not covered by the DPF — SCC, in accordance with the Atlassian DPA, on the basis of Article 46(2)(c) GDPR. Atlassian confirms the participation of its US entities in the DPF.
ClickUp	Mango Technologies, Inc.	USA	Standard Contractual Clauses (SCC) adopted by Commission Implementing Decision (EU) 2021/914, incorporated into the ClickUp data processing agreement (DPA), Annex 3 — legal basis: Article 46(2)(c) GDPR. Data Protection Addendum

Notion	Notion Labs, Inc.	USA	Standard Contractual Clauses (SCC) adopted by Commission Implementing Decision (EU) 2021/914, applied under the Notion data processing agreement (DPA) — legal basis: Article 46(2)(c) GDPR. Notion indicates the SCC as the safeguard for data transfers outside the EU.

b. as regards the provision of services related to communication, marketing, analytics and automation

Tool	**Provider / entity indicated in the documentation**	**Country of transfer**	**Mechanism for legalising the transfer of personal data outside the EEA**
Slack	Salesforce, Inc.	USA	Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data; in other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.
Loom	Loom, Inc., Atlassian group	USA	Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data; in other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where

			necessary, additional safeguards.
Riverside	Riverside.FM Ltd.	Israel	Article 45(1) GDPR — Commission Decision 2011/61/EU concerning the adequacy of data protection in Israel, to the extent covered by that decision. Further transfers to other countries require a separate basis
Twilio	Twilio Ireland Limited or Twilio Inc., depending on the terms of the contract	USA	Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data; where this basis does not apply: Article 46(2)(b) in conjunction with Article 47 GDPR — Twilio's approved binding corporate rules, if they cover the given service and transfer; then Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards. The order and scope are determined by the data processing agreement
Ringostat	Netpeak LTD	Ukraine, USA, United Kingdom	United Kingdom: Article 45(1) GDPR — the applicable Commission Implementing Decision (EU) 2021/1772 concerning the adequacy of data protection in the United Kingdom, as currently in force. Ukraine: Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together

			with a transfer impact assessment and, where necessary, additional safeguards. USA: Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data; in other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.
Apollo.io	ZenLeads, Inc., operating as Apollo.io	USA	Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data; in other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.
Instantly	Foo Monk, LLC, operating as Instantly.ai	USA	Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.
Mailforge	Salesforge OÜ	USA	The transfer to Salesforge OÜ in Estonia alone does not constitute

			a transfer outside the EEA. For further transfers to the USA: Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data; in other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.
Findymail	Peanuts SaaS Studio	the platform uses global service providers such as AWS (Amazon Web Services), Stripe, Cloudflare, Sentry and Slack. Some of these entities are based in the USA or process data on a global basis	The transfer to France and processing in Finland do not require a mechanism under Chapter V GDPR. For actual further transfers outside the EEA not covered by an adequacy decision: Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards
Clay	Clay Labs Inc.	USA	Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards. The mechanism provided for in the data processing agreement
Aimfox	SocialGrowth LLC FZ	United Arab Emirates	Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by

			Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.
Resend	Plus Five Five, Inc.	USA	Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data; in other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.
Microsoft Clarity	Microsoft Ireland Operations Limited; Microsoft Corporation participates in the processing	USA	Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data; in other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.
Meta Pixel	Meta Platforms Ireland Limited for the European region	USA	Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data; in other cases

			Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.
LinkedIn Insight Tag	LinkedIn Ireland Unlimited Company	USA	Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data; in other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.
TikTok Pixel	TikTok Technology Limited and TikTok Information Technologies UK Limited	United Kingdom. TikTok stores and processes data in data centres located, among others, in the USA and Singapore. In addition, for technical and operational purposes, data is accessible to entities affiliated with the platform in the following countries: United Kingdom, Switzerland, Brazil, Canada, Israel, Japan, South Korea, Malaysia, Philippines	For the United Kingdom, Switzerland, Brazil, Israel, Japan and South Korea: Article 45(1) GDPR — the relevant Commission adequacy decisions, within their scope. Canada: an adequacy decision only for the commercial organisations subject to PIPEDA that it covers. For countries without adequacy, including Singapore, Malaysia and the Philippines: Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards. For the USA: Article 45(1) GDPR —

			Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data; in other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.
X Ads	X Internet Unlimited Company — the controller indicated for the EU/EFTA/UK	USA and other countries in which it has infrastructure	For the USA: Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data; in other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards. For other countries: Article 45(1) GDPR — the relevant adequacy decision or an effective mechanism under Article 46 GDPR.
Ahrefs	Ahrefs Pte. Ltd.	Singapore	Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards. Module 2 or 3, depending on the client's role.

Similarweb	Similarweb Ltd.	Israel	Article 45(1) GDPR — Commission Decision 2011/61/EU concerning the adequacy of data protection in Israel, to the extent covered by that decision.
Zapier	Zapier, Inc.	USA	Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data; in other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.
Make	Celonis group: Celonis Inc., Celonis SE and subsidiaries	USA	Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards. The relevant module according to the contract, including Module 2 for the controller–processor relationship.
Airbyte	Airbyte, Inc.	USA	Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.
trigger.dev	API Hero Ltd	United Kingdom	United Kingdom: Article 45(1) GDPR — the applicable Commission Implementing Decision (EU) 2021/1772

			concerning the adequacy of data protection in the United Kingdom, as currently in force. Further transfers not covered by adequacy: Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.
n8n	n8n GmbH	Germany (EEA)	The transfer to n8n GmbH in Germany and processing in the EEA do not require a mechanism under Chapter V GDPR. Further transfers: Article 45(1) GDPR — the relevant adequacy decision; for the USA, Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data; in other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment and, where necessary, additional safeguards.

c. as regards the provision of services related to AI, content creation, security and payments

Tool	**Provider/entity indicated in the documentation**	**Country of transfer**	**Mechanism for legalising the transfer of personal data outside the EEA**
ChatGPT	OpenAI Ireland Ltd for the EEA; within the group OpenAI OpCo, LLC	USA	Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US

			Data Privacy Framework, if the specific recipient in the USA holds active certification covering the transferred data; in other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with a transfer impact assessment (TIA) and, where necessary, additional safeguards.
Claude / Anthropic	Anthropic Ireland, Limited for the European region; Anthropic PBC	USA	Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, incorporated into the data processing agreement for services covered by commercial terms; the controller–processor or processor–processor module respectively. The transfer of data to Anthropic Ireland, Limited does not in itself constitute a transfer outside the EEA; the mechanism concerns the further transfer of data outside the EEA
OpenRouter	OpenRouter, Inc.	USA	Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, provided for in the data processing agreement concluded with OpenRouter, Inc.
Lovable	Lovable Labs Sweden AB / Lovable Labs Incorporated	USA	Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, incorporated into the data processing agreement for transfers not covered by an adequacy decision.

Cursor	Anysphere, Inc.	USA	Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, provided for in the Anysphere, Inc. data processing agreement; the appropriate module should be matched to the parties' roles.
Windsurf	Cognition AI, Inc.	USA	Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914. Cognition AI, Inc. indicates the clauses as the mechanism for transfers of European data.
Browser Use	Browser Use Inc.	USA	Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, incorporated into the Browser Use data processing agreement for transfers requiring appropriate safeguards.
Z.ai	Jingsheng Hengxing Technology Pte. Ltd.	Singapore	For the transfer to Singapore, the basis is Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914.
ElevenLabs	Eleven Labs Inc.; the group also includes companies in other countries	USA	For the transfer to a recipient in the USA: Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the transferred data. In other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission

			Implementing Decision (EU) 2021/914, in accordance with the data processing agreement.
Higgsfield	Higgsfield Inc.	USA	Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914. The policy indicates the possibility of applying the clauses and an adequacy decision, but its general declarations do not confirm that the clauses have been effectively concluded with the client. Article 45(1) GDPR and Commission Implementing Decision (EU) 2023/1795 may be relied on for a US recipient only after confirming active certification and its scope
arcads.ai	FRESHR, a French SAS company	USA	The transfer of data to FRESHR in France does not constitute a transfer outside the EEA. For further transfers: Article 45(1) GDPR — the relevant Commission decision stating an adequate level of protection; for a recipient in the USA, Commission Implementing Decision (EU) 2023/1795 only where there is active certification covering the data. In other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, after confirming their application to the specific sub-processor or integration
Adobe	Adobe Systems Software Ireland Limited for users outside North America and Japan	USA, India	For transfers to a certified recipient in the USA: Article 45(1) GDPR — Commission Implementing Decision

			(EU) 2023/1795 concerning the EU–US Data Privacy Framework, provided there is active certification covering the data. In other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, applied in the relevant relationships within the group and with providers. Adobe indicates the clauses and adequacy decisions also for transfers carried out by the Irish company.
Canva	Canva Pty Ltd	Australia, USA	For transfers to Australia: Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, provided for in the Canva data processing agreement for transfers requiring safeguards. Australia is not covered by a Commission adequacy decision. The basis for further transfers should be determined according to the country and the specific recipient.
Figma	Figma, Inc.	USA	Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient in the USA holds active certification covering the transferred data. For transfers not covered by this basis: Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, in accordance with the

			relevant contractual documentation
Filmora	Wondershare Technology Group Co., Ltd. and subsidiaries	USA, China, Singapore	Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, after confirming their application to the relevant Wondershare company and the given transfer.
Magnific / Freepik	Freepik Company, S.L.	USA and other countries in which the providers of external artificial intelligence models and of cloud and analytics services are located	The transfer of data to Freepik Company, S.L. in Spain does not constitute a transfer outside the EEA. The mechanism for further transfers requires confirmation for specific recipients: Article 45(1) GDPR — the relevant decision stating an adequate level of protection, or Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914.
LastPass	LastPass Ireland Limited, LastPass UK Ltd and LastPass US LP — the entities indicated as joint controllers	USA, United Kingdom	For transfers to the USA: Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the data; in other cases Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914. For transfers to the United Kingdom: Article 45(1) GDPR — the applicable Commission decision concerning the adequate level of protection in the United Kingdom. The transfer to the Irish

			company remains within the EEA
Stripe	Stripe Technology Company, Limited; for part of the services, Stripe Technology Europe, Limited	USA	The transfer of data to the indicated Irish companies does not constitute a transfer outside the EEA. For further transfers to the USA: Article 45(1) GDPR — Commission Implementing Decision (EU) 2023/1795 concerning the EU–US Data Privacy Framework, if the specific recipient holds active certification covering the data. For transfers not covered by an adequacy decision: Article 46(2)(c) GDPR — Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, in accordance with the relevant transfer annex.

3. The possibility of transferring data concerns both sending it to recipients located outside the EEA and enabling such recipients to access data stored in the EEA remotely, in particular as part of technical support or the use of further processors. Storing data on a server in the European Union does not preclude such a transfer.

4. The Joint Controllers transfer data outside the EEA only where an appropriate legal basis for processing is ensured and the requirements of Chapter V GDPR are met. The transfer takes place:
    a. **on the basis of Article 45 GDPR** — if the specific transfer is covered by a European Commission decision stating an adequate level of data protection,
    b. **on the basis of Article 46 GDPR** — if the transfer is not covered by such a decision, with the application of appropriate safeguards, in particular the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
5. Where data is transferred to the United States, the basis for the transfer may be Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 concerning the EU–US Data Privacy Framework. This basis may be relied on only where the specific recipient holds current certification and the transferred data and the given transfer are within its scope. In other cases, the Joint Controllers ensure another appropriate basis for the transfer. The list of these organisations has been published by the U.S. Department of Commerce. Transferring personal data from the EEA to organisations that have joined the „EU–US Data Privacy Framework" programme and are on that list is possible without the need to obtain additional authorisations or to apply legal instruments such as Standard Contractual Clauses or binding corporate rules. However, where a given data importer in the USA has not joined the „EU–US Data Privacy Framework" programme, transferring personal data to it is possible and will take place after the conditions set out in Article 46 or 49 GDPR have been met. In such cases, the Joint Controllers will rely on the EU Standard Contractual Clauses and other safeguards in order to enable transfers outside the EEA. For transfers based on Standard Contractual Clauses, the Joint Controllers assess the effectiveness of the safeguards adopted, taking into account the circumstances of the transfer and the law and practice of the destination country. Where necessary, they apply additional technical, organisational or contractual measures. If the required level of protection cannot be ensured, the transfer is not commenced or is suspended.
6. The exceptions set out in Article 49 GDPR may be applied only in specific situations, after the conditions appropriate for the given exception have been met. They do not constitute a standard basis for the permanent transfer of data in connection with the use of foreign providers.
7. Information on the destination countries, recipients and bases for transferring data in connection with a specific service, as well as a copy of the appropriate safeguards, can be obtained by contacting the Joint Controllers of Personal Data at the following e-mail address: gdpr@mta.digital.

8. The Joint Controllers may make anonymised data (i.e. data that does not identify specific Users) available to external service providers in order to better recognise the attractiveness of advertisements and services for users, and in this respect, due to the registered office of the software providers, data may be transferred – while maintaining the principles of its protection – to third countries that nevertheless ensure compliance with the Standard Contractual Clauses approved by the European Commission in the field of personal data processing, or that have the relevant authorisations to act in this way on the basis of bilateral data processing agreements between the European Union and the given third country that is not a member of the European Economic Area. In the case of the Joint Controllers, these entities are:
    a. Google LLC for the Google Analytics tool used to analyse website statistics, Google Tag Manager: used to manage scripts by easily adding code snippets to a website or application and tracking actions performed by users on the website, Google Ads used to display sponsored links in the results of the Google search engine and on partner pages within the Google AdSense programme, Google Workspace allowing for comprehensive website editing and coordination of the work of the people working on it (including Google Drive, Gmail, Google Sheets, Google Forms, Google Looker Studio); More information on how Google Analytics collects and uses data can be found on the official Google page at: www.google.com/policies/privacy/partners. In addition, each User may prevent Google from collecting and processing data concerning their use of the website by downloading and installing the browser plug-in available at the following link: http://tools.google.com/dlpage/gaoptout.
    b. Meta Platforms, Inc. for the Facebook pixel used to track conversions from Facebook advertisements, optimise them on the basis of the collected data and statistics, and build an audience list targeted at future advertisements.
    c. Microsoft Ireland Operations Ltd. for the Microsoft Clarity tool used to analyse how the user interacts with the website through session recordings, heatmaps and traffic statistics.
    d. LinkedIn Ireland Unlimited Company for the LinkedIn Insight Tag tool used to track conversions, optimise advertising campaigns and build audiences on the LinkedIn portal.
    e. TikTok Technology Limited for the TikTok Pixel tool used to measure the effectiveness of advertisements, optimise marketing content and tailor offers on the TikTok platform.
    f. X Corp. (formerly Twitter) for the X Ads (Twitter Pixel) tool used to monitor user actions after advertisements are displayed on the X portal and to personalise marketing messages.
9. The Joint Controllers take all necessary measures to ensure that their subcontractors and other cooperating entities also guarantee the application of appropriate security measures whenever they process personal data on behalf of the Joint Controllers.
10. In accordance with the judgment of the Court of Justice of the European Union of 16 July 2020, the Joint Controllers continue to assess the legal system of the countries to which data is transferred and, where necessary, update the measures intended to ensure appropriate levels of protection.
11. As regards data transferred to the United States, the Joint Controllers, when making data available to third parties, make every effort to ensure that this takes place, in accordance with the European Commission decision of 10 July 2023, only to entities and organisations in the USA that ensure compliance with the new „EU–US Data Privacy Framework". In addition, in connection with the use of the Aimfox tool (SocialGrowth LLC FZ) based in the United Arab Emirates, personal data may be transferred outside the European Economic Area to a third country not covered by a European Commission decision stating an adequate level of protection, nor by the „EU–US Data Privacy Framework" programme. In such a case, the Joint Controllers base the transfer of data on the Standard Contractual Clauses approved by the European Commission and on other safeguards ensuring an appropriate level of personal data protection.

§ 5. Automated decision-making, including profiling

The Joint Controllers use, in their activity, tools based on artificial intelligence (AI), in order to optimise work, create transcriptions of meetings and generate summaries. We inform you that the processing of personal data by means of these tools is of a purely auxiliary nature and does not involve automated decision-making producing legal effects concerning Users or similarly significantly affecting them (in accordance with Article 22 GDPR). Furthermore, the Joint Controllers ensure that personal data entered into approved AI systems within cloud environments (e.g. Google Workspace) is not used by the providers of these services to train their own, public language models.

§ 6. User's rights

1. A User whose personal data is processed has the right to:
    a. **access, rectification, restriction, erasure or portability** - the data subject has the right to request from the Joint Controllers access to their personal data, its rectification, erasure („right to be forgotten") or restriction of processing, and has the right to object to processing, as well as the right to data portability. The detailed conditions for exercising the rights indicated above are set out in Articles 15-21 of the GDPR.
    b. **withdrawal of consent at any time** – a person whose data is processed by the Joint Controllers on the basis of consent given (on the basis of Article 6(1)(a) or Article 9(2)(a) of the GDPR) has the right

to withdraw consent at any time without affecting the lawfulness of the processing carried out on the basis of consent before its withdrawal.

c. **lodging a complaint with a supervisory authority** – a person whose data is processed by the Joint Controllers has the right to lodge a complaint with a supervisory authority in the manner and procedure specified in the provisions of the GDPR and Polish law, in particular the Personal Data Protection Act. The supervisory authority in Poland is the President of the Personal Data Protection Office in Warsaw.

d. **objection** - the data subject has the right to object at any time – on grounds relating to their particular situation – to the processing of personal data concerning them based on Article 6(1)(e) (public interest or tasks) or (f) (legitimate interest of the controller), including profiling on the basis of those provisions. In such a case, the Joint Controllers may no longer process that personal data unless they demonstrate the existence of compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or grounds for the establishment, pursuit or defence of claims.

e. **objection concerning direct marketing** - if personal data is processed for the purposes of direct marketing (based on the legitimate interest of the Joint Controllers, not on the basis of the data subject's consent), the data subject has the right to object at any time to the processing of personal data concerning them for the purposes of such marketing, including profiling, to the extent that the processing is related to such direct marketing.

2. The above rights are exercised on the basis of the user's request sent to the e-mail address: gdpr@mta.digital
3. The above rights are exercised taking into account the exceptions and limitations provided for in the GDPR, in particular the limitations of the right to erasure (Article 17(3) GDPR — e.g. where further storage is necessary to comply with a legal obligation, such as the 5-year retention of accounting documentation, or for the establishment, pursuit or defence of claims) and the limitations of the right to object (Article 21(6) GDPR). If we cannot fully comply with a request, we will explain the basis for the limitation within the 30-day period required by Article 12(3) GDPR.

§ 7. The right to lodge a complaint with a supervisory authority

If the processing of personal data infringes the provisions of the law, you have the right to lodge a complaint with a supervisory authority regarding the processing of personal data by the Joint Controllers of Personal Data. A complaint may be lodged with the President of the Personal Data Protection Office (the Office of the President of the Personal Data Protection Office is located in Warsaw (00-014), at ul. Moniuszki 1A).

§ 8. Cookies

„Cookies" are to be understood as IT data, in particular text files, stored on users' end devices (usually on the computer's hard drive or on a mobile device) used to save, by the user's browser, specific settings and data for the purpose of using websites. These files make it possible to recognise the user's device and display the website appropriately, ensuring comfort during its use. Storing „cookies" therefore makes it possible to appropriately prepare the website and offer according to the user's preferences - the server recognises the user and remembers, among other things, preferences such as: visits, clicks, previous actions.
A full, continuously updated list of the cookies used on the Joint Controllers' websites — including the file name, provider, purpose, category (necessary, preferential, statistical/analytical, marketing/advertising) and retention period — is generated automatically by the Cookiebot platform and is available in the consent management panel (Cookie Banner) on each of the sites. Because the list refreshes automatically when tools are added or removed, we do not keep a static numerical summary of it in the text of the Policy; the current data is always visible in the Cookiebot panel.
By using the website made available at the domain https://mta.digital/, https://www.anchor.team/, https://www.sharkpress.agency/, https://forceofnatu.re/, https://zerofluff.digital/, https://metrics.agency/, https://nodash.pl/, anchor-watch-ai or https://mtacu.pl/, consent is given to the installation of so-called necessary cookies on the end device of the person using the Site. Giving consent to the installation of necessary cookies is a precondition for using the Joint Controllers' website. With regard to the other categories of cookies, the user has the possibility to give consent to their use by the Joint Controllers, which, however, is not a condition for using the Joint Controllers' website. With regard to cookies other than necessary ones, consent is given by means of the web browser settings. If the User does not agree to the use of cookies other than necessary ones, they should change their browser settings accordingly or refrain from using the Site (more information below). The aforementioned action will not, however, make it impossible to use the Joint Controllers' website.
The table below presents the types of cookies used by the sites https://mta.digital/, https://www.anchor.team/, https://www.sharkpress.agency/, https://forceofnatu.re/, https://zerofluff.digital/, https://metrics.agency/, https://nodash.pl/, anchor-watch-ai and https://mtacu.pl/, together with additional information on the purpose of each of them.

Type of cookie	Characteristics

Session cookies	These cookies serve to process information enabling the user's session to be maintained until the web browser is closed. In principle, session cookies do not collect personal data in a way that would allow direct identification of the user. Their main task is to store information about the current browsing session, such as the contents of a shopping cart in an online store or the login status. However, in certain situations, the information collected by cookies, combined with other data, may potentially lead to the identification of a person.
Persistent cookies	These cookies make it possible to personalise services for Users – saving search criteria. Long-term cookies may potentially collect personal data.
Third-party cookies	These cookies are placed by third parties. In the case of our site, this is the provider of the Cookiebot tool. More information on the processing of personal data by the Cookiebot tool can be found at the following link https://www.cookiebot.com/en/privacy-policy/. Although cookies do not directly store a first name and surname, e-mail address or telephone number, they may nevertheless identify the user via IP address, device ID or other unique identifiers. This data, combined with other information collected by cookies, may be used to create a user profile and track their activity online.

Type of cookie	Characteristics
Necessary/Essential cookies	Necessary cookies contribute to the usability of the site by enabling basic functions such as navigation on the site and access to secure areas of the website. The website cannot function properly without these cookies. Necessary cookies, as a rule, do not collect personal data in a way that would allow the identification of a specific person. Although they do not collect personal data, in some cases, combined with other information, they may potentially contribute to the identification of the user
Preference cookies	Preference cookies make it possible for the site to remember information that changes the way the site looks or behaves, e.g. the preferred language or the region in which the user is located. Preference cookies, such as those remembering language or display settings, may collect personal data.
Statistical/Analytical cookies	Statistical cookies help website owners understand how different users behave on the site by collecting and reporting anonymous information. Cookies make it possible to count visits to the websites of the Joint Controllers of personal data and traffic sources, count the number of users and thereby measure and statistically analyse how Users use the site. The aforementioned cookies may potentially collect personal data in the form of so-called behavioural data, i.e. data on how the website is used, which may be considered personal data.
Marketing/ Advertising cookies	Marketing cookies are used to track users across websites. The aim is to display advertisements that are relevant and interesting for individual users and thereby more valuable for third-party publishers and advertisers. These files collect information about the user's behaviour obtained while browsing the site, in order to display advertisements related to their browsing profile. The aforementioned cookies may collect information about the location, preferences, browsing history and behaviours of users, which may also be considered personal data.
Unclassified cookies	Unclassified cookies are files that are in the process of being classified, together with the providers of the individual cookies.

The information stored in cookies within the websites is used by the Joint Controllers, with the exception of the files defined as „third-party cookies". Third-party cookies are cookies used and managed by external entities in order to provide the services we require in order to improve our services and the User's experience while browsing our website. The main services for which third-party cookies are used are obtaining access statistics.
As part of cookie technology, the Joint Controllers may use tracking pixels or clear GIF files in order to collect information about how the user uses their services and their reactions to marketing messages sent by electronic mail.
The Joint Controllers may use internet log files (which contain technical data, such as the user's IP address) in order to monitor traffic within their services, resolve technical problems, detect and counteract fraud, and enforce the rules for using the Joint Controllers' services.
The Joint Controllers do not use any cross-site tracking technologies, and the personal data collected concerning each user is not sold or made available by them for the purposes of advertising based on the collection of cross-context behaviours from various websites.
The Joint Controllers inform you that the site does not respond to DNT (Do Not Track) signals, but the user may disable certain forms of online tracking, including some analytics data and personalised advertisements, by changing the cookie settings in their browser or by means of our cookie consent tools (if applicable).
Detailed information on changing the settings concerning Cookies and on deleting them yourself in the most popular web browsers is available in the help section of the web browser and on the following pages (just click on the given link):

1. Google Chrome
2. Mozilla Firefox
3. Microsoft Edge
4. Opera
5. Safari macOS
6. Safari iOS/iPad OS

Detailed information on managing cookies on a mobile phone or other mobile device should be found in the user manual of the given mobile device.

§ 9. B2B direct marketing (outreach)

1. The provisions of this paragraph apply only to the extent that a given Joint Controller actually conducts B2B direct marketing activities (so-called outreach), i.e. independently initiates commercial contact with entrepreneurs who have not previously approached the Joint Controller. These provisions supplement § 1–8, which govern the other matters (including individuals' rights, cookies and the procedure for lodging complaints).
2. Legal basis. The basis for processing is the legitimate interest of the Joint Controller consisting in conducting B2B direct marketing (Article 6(1)(f) GDPR; recital 47 GDPR expressly indicates direct marketing as an example of such an interest). A balancing test (LIA) is carried out and periodically reviewed.
3. Scope of data. We process only data related to business activity: first name and surname (if publicly available), business e-mail address, position/role, company name, URL of a public profile (e.g. LinkedIn), public information about the company, and the history of communication with us.
4. Sources of data (Article 14 GDPR). We obtain data exclusively from publicly available sources, in particular: public registers (KRS, CEIDG), websites and public professional profiles (e.g. LinkedIn), public B2B databases and contact acquisition tools (Apollo, Clay, Findymail, Prospeo, Instantly), public materials (podcasts, conferences) and public technical registers (e.g. Certificate Transparency logs, crt.sh). Upon a request sent to gdpr@mta.digital, we will indicate the source of specific data within 30 days (Article 12(3) GDPR).
5. Retention period. The data of persons with whom we conduct correspondence or who have not responded — up to 24 months from the last contact. After an objection is lodged, the data is placed on an exclusion list and is stored solely in order to avoid repeated contact. Upon an explicit request, we erase the data earlier — at the latest within 30 days.
6. Objection and opt-out. You can opt out of outreach: by replying to the message with the word STOP or „I am not interested", by clicking the opt-out link in the message footer, or by writing to gdpr@mta.digital. The opt-out is carried out without delay, at the latest within 30 days; after it is submitted, the data remains solely on the exclusion list in order to prevent repeated contact.
7. Automated qualification (Article 22 GDPR). For the purposes of certain campaigns, we may use an automated analysis of the match between a company and our offer based on public data. This is not automated decision-making producing legal effects or similarly significantly affecting a person within the meaning of Article 22(1) GDPR — the only effect is whether we send a message at all. You retain the right to obtain human intervention, to express your own point of view and to contest the result (gdpr@mta.digital).
8. Sole traders (Electronic Communications Law). With regard to addressees who are natural persons conducting sole proprietorship business activity (entered in CEIDG), we additionally apply the rules arising from the Electronic Communications Law (PKE). We direct cold contact to the data published by the addressee in a B2B context (company website, public professional profile, public registers) on the basis of Article 6(1)(f) GDPR; where consent is the more appropriate basis, we obtain it before sending the message.

Contact via WhatsApp (if applicable). If you provide a telephone number and separately tick consent to contact via WhatsApp, we may send you one message concerning your enquiry. The basis is your consent (Article 6(1)(a) GDPR in conjunction with Article 398 PKE). The recipient is WhatsApp Ireland Ltd / Meta Platforms Ireland Ltd. You may withdraw consent at any time (reply STOP), without affecting the lawfulness of the earlier processing.

9. Open tracking. Outreach messages may contain pixels measuring opens — solely for the purposes of campaign effectiveness statistics; we do not combine this data with external profiles, nor do we build individual recipient profiles on its basis.
10. Contact for outreach matters: gdpr@mta.digital.

§ 10. Data security

1. The Joint Controllers apply appropriate technical and organisational measures ensuring the security of the processed personal data, appropriate to the risk of infringement of the rights or freedoms of natural persons and to the nature and scope of the processed data.
2. The measures applied are intended to protect data against loss, destruction, accidental or unlawful disclosure, making it available to unauthorised persons, alteration or unauthorised access. Depending on the nature of the processing, measures applied include, among others, encryption, SSL/TLS certificates, data transmission safeguards and mechanisms for controlling and restricting access to systems.
3. The Joint Controllers apply procedures for detecting, assessing, documenting and handling incidents related to data security. In the event of an incident occurring or being suspected, they take action aimed at limiting its effects, securing data and evidence, establishing the causes and scope, and preventing it from recurring.
4. In the event of a personal data breach being established, the Joint Controllers carry out an assessment of the risk to the rights and freedoms of natural persons and, in the cases required by law, report the breach to the supervisory authority and notify the data subjects.
5. The Joint Controllers regularly assess the security measures applied and, where necessary, update them, adapting them to changing threats and technological solutions.
6. The content of this Privacy Policy was updated as at 13 October 2026.