

USER BEHAVIOR ANALYTICS **UBA NETWORKS** UNIFIED VISUAL SECURITY

Privacy Policy

Who we are?

This Privacy Policy aims to give you information on how UBA Networks collects and processes your personal data through your use of the website at www.ubanetworks.com, including any data you may provide to us through this website. This information is collected and processed when you contact us to leave questions or feedback or when you sign up for our email newsletters.

This website is not intended for children and we do not knowingly collect data relating to children.

It is important that you read this Privacy Policy together with any other policy or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This Privacy Policy supplements the other notices and is not intended to override them.

Who controls your data?

UBA Networks is the controller and is responsible for your personal data (referred to as “UBA Networks”, “we”, “us” or “our” in this Privacy Policy).

We have appointed a data privacy manager who is responsible for overseeing questions in relation to this Privacy Policy. If you have any questions about this Privacy Policy, including any requests to exercise your legal rights, please contact the Data Privacy Manager using the details set out below.

Our full details are:
UBA Networks AB
Data Privacy Manager
dpo@ubanetworks.com

Beväringsgatan 7

703 65, Örebro

Sweden

You have the right to make a complaint at any time to datainspektionen supervisory authority for data protection issues (www.datainspektionen.se). We would, however, appreciate the chance to deal with your concerns before you approach the ICO (information commissioner officer) so please contact us in the first instance.

Third-party links

This website may include links to third-party websites, plug-ins, and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy policy or other relevant information on every website you visit.

What we collect

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store, and transfer different kinds of personal data about you which we have grouped together follows:

- **Identity Data** includes first name, last name, username, and any other personal details you may send to us.
- **Contact Data** includes an email address.
- **Technical Data** includes internet protocol (IP) address, browser type, and version, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access this website.
- **Usage Data** includes information about how you use our website and how you view the emails we send you including which links you click on.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We also collect, use, and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does not directly or indirectly reveal your identity. If Aggregated Data is combined with personal data, it will only be treated in line with this Privacy Policy.

We will only collect **Special Categories of Personal Data** about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data) for the purposes of exercising our specific rights with respect to employment as permitted under the applicable legislation. If you provide us with this information, for example as part of your application for a job, you agree that we may collect and process these Special Categories of Personal Data for these purposes only. We will always exercise these rights in accordance with the applicable law and will use all appropriate safeguards in order to protect your interests.

How we collect your data

We use different methods to collect data from and about you including through:

- **Direct interactions.** You may give us your Identity and Contact Data by filling in forms or by corresponding with us by post, phone, email, or otherwise. This includes the personal data you provide when you:
 - create an account on our website;
 - subscribe to our service or publications;
 - request marketing to be sent to you;
 - enquire about a job; or
 - give us some feedback.
- **Automated technologies or interactions.** As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions, and patterns. We collect this personal data by using cookies, server logs, and other similar technologies.
- **Third parties or publicly available sources.** We may receive personal data about you from various third parties as set out below:
 - Technical Data from analytics providers such as Google based outside the EU;

How we use your data

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances: - Where we need to perform the contract we are about to enter into or have entered into with you. - Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. - Where we need to comply with a legal or regulatory obligation.

Generally, we do not rely on consent as a legal basis for processing your personal data other than in relation to sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us at contact@ubanetworks.com

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

We may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please [contact us](#) if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	Type of data	Lawful basis for processing including the basis of legitimate interest
To register you as a new customer	(a) Identity (b) Contact	Performance of a contract with you
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy; (b) Asking you to leave a review or take a survey; (c) Sending you our newsletter.	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)
To evaluate your eligibility for new or existing jobs	(a) (Identity) (b) (Contact) (c) Special Categories of Personal Data	Necessary for our legitimate interests (for running our business and operating our recruitment practices)
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting, and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganization or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business, and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, customer relationships, and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business, and to inform our marketing strategy)
To make suggestions and recommendations to you about goods or services that may be of interest to you	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile	Necessary for our legitimate interests (to develop our products/services and grow our business)

Explanation of Lawful Basis

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by [contacting us](#).

Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal or regulatory obligation means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

Marketing

We will make every effort to provide you with choices regarding certain personal data uses, particularly around marketing and advertising.

We may use your Identity, Contact, Technical, Usage, and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services, and offers may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us, purchased services from us or if you provided us with your details when you subscribed to our newsletter and, in each case, you have not opted out of receiving that marketing.

We won't share your information with any other organizations for marketing, market research, or commercial purposes, and we don't pass on your details to other websites.

Opting out

You can ask us or third parties to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you or by [contacting us](#) at any time.

Where you opt-out of receiving these marketing messages, this will not apply to personal data provided to us as a result of a service purchase, service experience, or other transaction.

Cookies

UBA Security puts small files (known as 'cookies') onto your computer to collect information about how you browse the site.

Cookies are used to:

- Measure how you use the website so it can be updated and improved based on your needs; and
- Remember the notifications you've seen so that we don't show them to you again.

Below is a table of the cookies we use, what we use them for, and how long they will be stored on your computer:

Name	Cookie	Purpose	Expires
Google Analytics	_gat_gtag_UA_[id]	This lets us distinguish users.	Session
Google Analytics	_ga	Used to distinguish users.	2 years
Google Analytics	_gat	Used to throttle request rate.	1 minute
Google Analytics	_gid	Used to distinguish users.	2 years
Google Analytics	_utma	This lets us know if you've visited before, so we can count how many of our visitors are new to www.ava.uk or to a certain page.	2 years
Google Analytics	_utmtb	This works with _utmc to calculate the average length of time you spend on www.ava.uk	30 minutes
Google Analytics	_utmc	This works with _utmb to calculate when you close your browser.	When you close your browser
Google Analytics	_utmz	This tells us how you reached www.ubanetworks.com (for example from another website or a search engine).	6 months
LinkedIn	UserMatchHistory	LinkedIn Ads ID syncing	30 days
LinkedIn	lang	Sets default locale/language	Session
LinkedIn	lissc	Tracking the use of embedded services.	1 year
LinkedIn	lids	Used for routing	1 day
LinkedIn	bcookie	Browser ID cookie	2 years
LinkedIn	bscookie	Secure Browser Cookie	2 years
Hubspot	__hssc		
Hubspot	__hs_opt_out		
Hubspot	__hs_initial_opt_in		

Name	Cookie	Purpose	Expires
Hubspot	hubspotutk	This cookie keeps track of a visitor's identity. It is passed to HubSpot on form submission and used when deduplicating contacts. It contains an opaque GUID to represent the current visitor.	13 months
Hubspot	__hsrc	Determine if the visitor has restarted their browser. If this cookie does not exist when HubSpot manages cookies, it is considered a new session. It contains the value "1" when present.	Session
Hubspot	__hstc	The main cookie for tracking visitors. It contains the domain, utk, initial timestamp (first visit), last timestamp (last visit), current timestamp (this visit), and session number (increments for each subsequent session).	13 months
Hubspot	messagesUtk	Recognize visitors who chat with you via the chat flows tool. If the visitor leaves your site before they're added as a contact, they will have this cookie associated with their browser. If you chat with a visitor who later returns to your site in the same cookies browser, the chat flows tool will load their conversation history. The cookie is controlled by the Consent to collect chat cookies setting in your chat flow. It contains an opaque GUID to represent the current chat user.	13 months
Cloudflare (via Hubspot)	__cfuid	This cookie is set by HubSpot's CDN provider because of their rate limiting policies .	Session
Cloudflare (via Hubspot)	__cfduid	This cookie is set by HubSpot's CDN provider, Cloudflare. It helps Cloudflare detect malicious visitors to the www.ubanetworks.com website and minimizes blocking legitimate users. The cookie is used to identify individual clients behind a shared IP address and apply security settings on a per-	Session

Name	Cookie	Purpose	Expires
		client basis. It is necessary for supporting Cloudflare's security features.	
AdRoll	__adroll	Registers a unique ID that identifies a returning user's device. The ID is used for targeted ads.	1 year
AdRoll	__adroll_fpc	Used to identify the visitor across visits and devices. This allows the website to present the visitor with relevant advertisement - The service is provided by third-party advertisement hubs, which facilitate real-time bidding for advertisers.	1 year
AdRoll	__ar_v4	Optimizes ad display based on the user's movement combined and various advertiser bids for displaying user ads.	1 year

Our cookies aren't used to identify you personally.

When we might change how we use your data

We will only use your personal data for the purposes for which we collected it unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please [contacting us](#).

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process or disclose your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Transferring your data

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries.

- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. For further details, see European Commission: Model contracts for the transfer of personal data to third countries.
- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between Europe and the US. For further details, see European Commission: EU-US Privacy Shield. UBA Security is aware that the European Court of Justice declared the EU–US Privacy Shield invalid on 16 July 2020 and we are in the process of revising our privacy policy.

Please [contacting us](#) if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

Your security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used, or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors, and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

How long we will use your data

We will only retain your personal data for as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data, and whether we can achieve those purposes through other means, and the applicable legal requirements.

By law, we have to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for six years after they cease being customers for tax purposes. With respect to information you provide to us in relation to an application for a job, we may keep this information for up to twelve years to make the processes by which we evaluate and assess candidates more efficiently.

In some circumstances you can ask us to delete your data: see below for further information.

In some circumstances, we may anonymize your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

Your rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data. You have the right to:

- **Request access** to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us to continue to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which overrides your rights and freedoms.
- **Request restriction of processing** of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data’s accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- **Request the transfer** of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- **Withdraw consent at any time** where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the rights set out above, please [contact us](#).

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response. We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.