
September 2024

Ativion Privacy Policy

www.Ativion.com

The logo for Ativion, featuring the word "ATIVION" in a bold, white, sans-serif font. The letter "A" is stylized with a diagonal slash through it. The background of the logo area is a large, light blue triangle pointing upwards, set against a darker blue background.

ATIVION



Ativion Privacy Policy

Effective and Last Updated: September 20, 2024

Who are we and what do we do?

The Ativion Group is a group of subsidiary companies of Impala Bidco and forms part of the Ativion and Netop companies as defined in our Group Structure available at www.ativion.com/legal/group-structure (referred to herein as “Ativion”, “us”, “we”, “ours”). Ativion operates www.ativion.com (the “Website”) and provides software and related services (“Services”). provide organizations (our “Customers”) with a secure and user-friendly way to monitor and manage the internal working of computer devices and how those devices are used by individuals operating under the control of the Customer (“Users”) and various individuals affiliated with a Customer (“Subjects”).

How this Privacy Policy applies to you

Thank you for reviewing Ativion’s privacy policy (“Privacy Policy”). This Privacy Policy tells you the types of information we collect about you and how we use your information when: (a) (1) you use our Websites or Services, (2) you are a potential Customer contact or (3) you purchase our Services, (b) how we use that information, and (c) the instances in which we share your information to others.

The Websites and our Services are not intended for use by children and, whilst we often process data relating to children on the instruction of our Customers, we do not knowingly collect data relating to children for our own purposes. Please note that where your personal data is uploaded onto our systems by a Customer for their use of our Services, they are the controller and responsible for that personal data, and you should consult them for details of how they will process your personal data. This Privacy Policy does not cover processing by us of such personal data.

Our Website and Services 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 and practices. When you leave our Website, we encourage you to read the privacy policy of every website you visit.

Our Services

Ativion provides Customers, and allows Customers to authorize Users to, access to the following software products (collectively, the “Services”):



- **Connect:** allows organizations to remotely access and control computer devices across a network and/or across the internet. This can be cloud-based or hosted. Connect processes Services Data, content of screen or display, and individual entered text (chat).
- **Webcheck:** product currently being phased out which offers robust internet filtering which analyses content in real-time to ensure Subjects are protected online. This is a solution powered by our partner, Netsweeper. This requires the processing of Services Data as well as some Special Category Data. You can view Netsweeper’s Privacy Notice at netsweeper.com/privacy-policy.
- **Content Keeper:** web filtering and security platform for schools. Unmatched cross-platform protection in the Cloud. Intelligent web filtering provides multiple layers of cross-platform intelligence that enable safety and security benefits, including real-time visibility, control of non-managed devices, filter circumvention and ransomware defense. Our web filter for schools uses AI categorization to analyze web traffic and automatically block web content containing pornography, substance abuse, extremism and other categories of sensitive and potentially harmful material. Reliable SSL inspection and granular domain controls eliminate over-blocking, so schools can provide safe access to popular domains including Vimeo, Google and YouTube that add value to learning. Provides parents the option to track logged student devices via the parent portal.
- **Backdrop:** core software which supports Wellbeing, Classroom and Safeguard modules.
 - **Wellbeing:** software to capture, record and identify signs of harmful online behavior. Users can highlight and prioritize Subjects of concern. This requires the processing of Services Data, contents of screen or display, as well as some Special Category Data which may be processed as part of screen captures which document device usage.
 - **Classroom:** software which makes it easy to monitor and manage student activity on classroom devices. This requires the processing of Services Data, contents of screen (including access to live screen displays) or display, and individual entered text (chat).
 - **Safeguard:** a school safety solution, allows schools to record, manage and track student mental health and safety concerns at any time by attaching students to an applicable incident for school configuration and management. This requires the processing of Services Data. Special Category Data may be processed when a Customer has linked to an organization’s Management or

Student Information System (MIS or SIS), or when a User enters such data manually. This information allows us to contextually provide safeguarding services. Any external referral by Users is logged in the system.

- Any use of information received from Google APIs will adhere to Google API Services User Data Policy, including the Limited Use requirements.”
- Education Pro: combines learner wellbeing and device management to enhance digital learning, support IT administration, manage classroom device usage, and monitor safeguarding issues effectively. Education Pro offers a range of hosting options and built-in cross-platform technology. This requires the processing of Services Data, contents of screen or display, and individual entered text (chat). Special Category Data may be processed as part of screen captures documenting device usage, and user entered data providing demographic information on individuals. Test modules provide individual scores associated with test questions for teacher administering the applicable test or quiz.
- **Edlink:** The EdLink software is a third-party solution which collects information around the location of the device and any applications or websites used as part of the normal use of the solution. The purpose of this data is to recover lost devices and perform control & monitoring functions on the target devices. This is powered by Mobile Guardian; their privacy policy can be found here:
<https://www.mobileguardian.com/privacy-policy/>.



- **Netop Vision** (including Netop Vision Pro, Netop Vision 365, Netop Vision for Chromebooks): software which makes it easy to monitor and manage student activity on classroom devices. This requires the processing of Services Data, contents of screen or display, and individual entered text (chat).

Who is responsible for the personal data which Ativion processes?

When providing our Services, Ativion acts as data processor on behalf of its Customers. Customers are responsible for providing appropriate privacy notices to Users and Subjects whose data they provide to us, explaining how their personal data will be processed and their rights in relation to it. Customers who provide an Ativion entity with sensitive categories of personal data need to comply with additional requirements under the local data protection laws of the territory in which they reside.

When you use an Ativion Service provided by your organization, Ativion’s processing of your personal data in connection with that Service is governed by a contract between Ativion and your organization. Ativion processes your personal data to provide the Service to your organization and you; we act on our Customers’ instructions in relation to the processing of personal data. We will comply with legal obligations in each territory where we provide services which are applicable directly to processors, including implementing appropriate technical and

organizational measures to ensure the security of the personal data.

The data we collect about you

In connection with the provision of our Website and during the sales process of our Services, we may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- **Identity Data** includes first name and last name, age, gender, home country, username or similar identifier and title.
- **Contact Data** includes name, company name, job title, physical address, email address, and telephone numbers.
- **Technical and Usage Data** includes information about how you access and use the Website and interact with us during your purchase and set up of our Services such as your internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our Website and Services, the pages you have visited and the links you have followed on them.
- **Profile Data** includes your username and password or similar identifiers; your job title; your employer; your searches using Customer devices with our Services; and your preferences, feedback, and survey responses.
- **Payment Data** includes your financial information such as credit card or debit card number or other financial information to make payments for the Services.
- **Employment Application Data** includes first name, last name, phone number, email address, physical address, employment history, and educational history.



- **Marketing and Communications Data** includes your preferences in receiving marketing from us and your communication preferences, your discussions with customer support, and any other communications or feedback you send us (including via email or social media).

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. For example, we may aggregate your Technical and Usage Data to calculate the percentage of Users accessing a specific Website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this Privacy Policy.

How is your personal data collected?

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

- **Direct interactions.** You may give us your Identity, Contact, Profile, Payment Data, and Marketing Communications Data when completing forms on our Websites, using our Services, or by corresponding with us by post, phone, email, social media, in person or otherwise. This includes personal data you provide when you:

- register to use our Services;
- complete a form on our Websites requesting us to contact you;
- request support services in relation to our products and Services;
- request marketing material to be sent to you;
- provide your details at an event or exhibition;
- complete a survey; or
- make a complaint, request or give us feedback.



- **Automated technologies or interactions.** As you interact with our Websites and Services, we may automatically collect Technical and Usage, and Profile, Data about your equipment, browsing actions and patterns. We may also collect this personal data by using cookies and other similar technologies.
- **Third parties.** We may receive Technical and Usage Data from third party analytics providers and Profile Data from third party analytics providers.

How we use your personal data

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. Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To register you as a new user of our products and/or Services and to provide our products and/or Services to your Users and Subjects	(a) Identity (b) Contact (c) Profile	Necessary for our legitimate interests (to be able to provide our Services to you, to provide specific features of our service to you, to improve and customize our service)



Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
<p>To manage our relationship with you which will includes: (a) Dealing with your enquiries, support requests and complaints;(b) Notifying you about changes to this Privacy Policy;(c) Asking you to leave a review or take a survey.</p>	<p>(a) Identity (b) Contact (d) Profile (e) Marketing and Communications</p>	<p>Necessary for our legitimate interests (to manage our user relationships and be able to provide and improve our Websites, products and Services</p>
<p>To administer and protect our Websites and Services (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)</p>	<p>(a) Identity (b) Contact (c) Technical and Usage</p>	<p>Necessary for our legitimate interests (for running our Websites and Services, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganization or group restructuring exercise) Necessary to comply with a legal obligation</p>
<p>To use data analytics to improve our Websites, products, Services, relationships with users and user experiences</p>	<p>(a) Technical and Usage</p>	<p>Necessary for our legitimate interests (to define types of users of our Websites, products and Services, to keep our Websites, products and Services updated and relevant, to develop our Websites, products and Services)</p>



Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To make suggestions and recommendations to you about our products, services, information and events that may be of interest to you	(a) Identity (b) Contact (c) Technical and Usage (d) Profile (e) Marketing and Communications	Necessary for our legitimate interests (to develop our Websites, products and Services)
To Personalize our Services for you	(a) Technical and Usage (b) Profile	For the Performance of the contract between us
To Consider your career application if you apply for a role with us	(a) Identity (b) Contact (c) Employment Application Data	For the Performance of the contract between us
To enable you to complete a survey	(a) Identity (b) Contact (c) Profile	Necessary for our legitimate interests (to study how users use our products and services and to develop them) You will provide your consent when entering the survey or competition



Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
Complete a transaction with us for Services, including to process payments and refunds and to deliver Services and any other information as requested	(a) Identity (b) Contact (c) Payment Data	For the Performance of the contract between us
To Detect, prevent, and address technical issues	(a) Technical and Usage	Necessary for our legitimate interests (to keep our Website and Services operating)
To Comply with laws and allow you to exercise your data privacy rights;	(a) Identity (b) Contact (c) Profile	It is our legal obligation to comply with the laws and allow you to exercise your data privacy rights
To provide you with marketing communications from us	(a) Identity (b) Contact	With your consent (which you may withdraw later)
For any purpose with your express consent	(a) Identity (b) Contact (c) Technical and Usage (d) Profile (e) Marketing and Communications	With your consent (which you may withdraw later)

Cookies

We may use cookies and similar technologies on our Website and our Services. This helps us to provide you with a good experience when you use our Websites and allows us to improve our Websites.

A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer if you agree. Cookies contain information that is transferred to your computer's hard drive.

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of our Services and Websites may become inaccessible or not function properly. Please see our Cookie Policy (available at www.ativion.com/legal/CookiePolicy) if you want further information on the specific cookies used by us.

Disclosures of your personal data

We may disclose your personal data for the purposes described above to the following third parties:

- **Our third-party service providers** who perform functions on our behalf in connection with the operation of our business such as IT service providers and system administrators, third parties who host and manage data, deliver our products and Services.
- **Professional advisers** including lawyers, bankers, auditors and others who provide consultancy, banking, legal, insurance and accounting services.
- **Law enforcement, government agencies, or other authorities** in order to comply with laws, regulations, court orders, or other legal



obligations, or to protect and defend our legal interests.

- **The institution** you are affiliated with, if you use our products through your affiliation with an institution, we may use your information to track activation of applications and to provide the Services.
- **Our third-party analytics partners** to analyze Website traffic and understand User needs and trends.
- **Third parties as required by law**, or if we believe that such action is necessary to: (a) fulfil a government, or regulatory authority request; (b) conform with the requirements of the law or legal process; (c) protect or defend our legal rights or property, Websites, Services or customers.
- **Third parties** to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this Privacy Policy.

We will require or endeavor to have all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions. Please see our Data Processors List available on our Website for more information.

International transfers

We are a global company with offices in the UK, US and Europe. We may share your personal data that we collect between our locations, and with service providers which help our operations. If we transfer your personal data out of the territory in which you are located, we ensure appropriate technical and security measures are in place.

Data 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. Every access or attempt to access personal data is logged and actively monitored. Although we have implemented industry measures to protect your data, we cannot guarantee that your data will be 100% secure when it is transmitted over the internet.

Data retention

We will only retain your personal data for as long as necessary to fulfil 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.

Atvion Privacy Policy September 2024



Your legal rights

Generally, we provide you with the following legal rights listed below. Please note that depending on the laws and regulations of where you live the rights listed below may not apply or may be different.

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 continuing to process it. 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 if you feel it impacts on your fundamental rights and freedoms. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms (other than in the case of direct marketing).

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.

Opting Out from Marketing Communications If you do not want to receive promotional or marketing communications from Ativion, you may opt-out of receiving those communications at any time. You may opt out of having your personal data collected by not signing up for Services, or creating an account. To opt out after submitting personal data, you must contact us at dpo@ativion.com or you may send us your request at <https://www.ativion.com/contact/>. We will endeavor promptly opt you out of any marketing communications.

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.

Ativion Privacy Policy September 2024



If you wish to exercise any of the rights set out above, please contact us.

No fee usually required 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 we determine that your request is objectively 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.

Time limit to respond 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. You have the right to make a complaint at any time to the supervisory authority for data protection issues. We would, however, appreciate the chance to deal with your concerns before you approach the relevant supervisory authority, so please contact us in the first instance.

For Residents of the European Economic Area and United Kingdom

If you are located in the European Union, Iceland, Liechtenstein or Norway (the

“European Economic Area” or “EEA”) or in the United Kingdom (“UK”), you are entitled to additional rights regarding our use of your personal data. To learn more, see the EU-UK Privacy Rights Notice.

For Residents of the State of California Privacy

If you are a California resident, California law may provide you with additional rights regarding our use of your personal data. To learn more about your California privacy rights, see California Privacy Rights Notice.



Changes to the Privacy Policy and your duty to inform us of changes

Ativion reserves the right to change this Privacy Policy at any time, without notice, by posting the new or revised Privacy Policy and the new revision date at a <https://www.ativion.com/legal/privacy-policy/>.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

Contact Us

If you have any questions about our Policy or any questions about how we use your Personal Data, please contact us at:

Impero Holdings Limited t/a Ativion

Email address: dpo@ativion.com

Postal address: Ativion, Seventh Floor, East West, Tollhouse Hill, Nottingham, UK, NG1 5FS

Webform: <https://www.ativion.com/contact>