Privacy policy

Oddity.ai

Last revision: February 18th 2020.

Oddity's mission is to bring public safety to a whole new level through human-machine collaboration. We believe personal safety and security is important. We also think the values of individual safety and security must be balanced with the right to privacy. As such, we always do our best to make sure we do not violate anyone's privacy in the process of catching the bad guys.

Contact

Oddity.ai B.V. offices are on the Gansstraat 170, 3582 EP, Utrecht in the Netherlands. Call us at +31614780971. E-mail us at hello@oddity.ai or contact our Data Protection Officer (DPO) at fg@oddity.ai.

Data collection on our website

This section describes our data collection practices with regards to our public website (oddity.ai). We may collect data when you use our services, or when you hand them over to us. We might collect (1) IP-addresses, (2) location data, (3) data about your activity on our website, (4) the webbrowser and device you use to visit our website.

We do not actively collect special personal data ("bijzondere persoonsgegevens" in Dutch law). We do not intend to collect any data on persons under the age of 16, but cannot guarantee as such. It is recommended that parents or guardians monitor the internet usage of their underage children. If you think we might have collected data of someone that is underage, please contact our Data Protection Officer so we can destroy such information as required by the General Data Protection Regulation of the European Union (GDPR).

Oddity collects data on its website for the purposes of improving our services and keeping information up to date as well as to guarantee high-quality content. Oddity does not make automated decisions based on the data collected on our website. Oddity keeps the collected information (1, 2, 3 and 4) as long as necessary, but no longer than strictly required and never longer than 26 months after the data was initially collected.

Oddity uses functional cookies to improve the workings of our website. Oddity places some cookies to track and monitor your behavior on our website through third-parties: Google Analytics, YouTube, crisp.chat, and formspree.io. All personal details (in accordance with the definition of "personal data" as defined in the GDPR) are destroyed and replace by anonymous tracking IDs. You can opt-out by setting up your browser such that it does not accept cookies from our domains (oddity.ai, *.oddity.ai).

Data collection through our research and development activities

This section describes our data collection practices as part of our research and development activities. Oddity develops machine learning algorithms that are "trained" using video data. Often, a reference set of videos of which it is known they depict some anomaly (like violence, fainting, etc.) and a set of various videos is used to "train" an algorithm to detect the anomaly on unknown data later. Oddity draws from public (academic and non-academic) sources to create these video-datasets. The data is unstructured. It is non-trivial to extract personal identifiable data from these datasets. The primary aim of the data collection process is to build datasets that can be used to improve our algorithms, and eventually help protect the safety of citizens, employees or other subjects of video surveillance systems on which Oddity's algorithms operate.

We do not actively collect special personal data ("bijzondere persoonsgegevens" in Dutch law). The video data we collect is treated as-is and no efforts are made to identify or track persons visible in it. Oddity's algorithms use the semantic information in it to learn to recognize activities rather than persons. Oddity does not identify persons, but identifies behavior. Apart from the training process, Oddity does not make any automated decisions with impact based on our dataset that affect you in any way.

The data collected through our research and development efforts is stored indefinitely, but no longer than strictly required to train our algorithm(s). Our datasets are constantly updated and adjusted to meet our highest quality standards and a subset of videos we collect are eventually tossed from the dataset. If you think video footage that can be used to identify you is part of our datasets, you can assert your rights as described in the last section ("Your rights") of this document.

Data collection through our commercial services

Oddity owns and operates physical and software installations that process and analyze live footage from video surveillance cameras such as those used by government and private industry. Oddity receives this data through third-parties (our customers) and is not ultimately responsible. Nonetheless, as required by European law, Oddity signs processing agreements with all third-parties that provide us with video feeds that might (indirectly) contain personal data. Oddity understands that the video data it collects is sensitive and must be handled with great care. We also believe that this responsibility requires transparency. As such, even though we are not strictly required to do so, this section summarizes the data collection practices we perform as third-party service provider for government and private industry. Please note that this section ("Data collection through our commercial services") is meant as a general description of how we process video data of which we are not the ultimate "owner", nor responsible for. This section has been included in the spirit of openness and transparency but is not legally binding. As written in European and international law, the ultimate controller is responsible for this data.

Oddity's systems processes and analyzes video footage that might be taken in public areas such as city centers, streets, industrial parks and others. Our customers mainly collect this data to ensure the safety of citizens, employees or visitors; some customers have other aims, please refer to their respective privacy policies to understand what data is collected and why. Government agencies might use video data to conduct criminal investigations (in accordance with law). Governmental institutions are bound by law to handle video surveillance data with great care. Private companies can only use video surveillance systems to monitor their own properties and must take all precautions necessary to prevent filming public areas such as (public) streets. Oddity is aware of the relevant laws and regulations surrounding video surveillance and holds itself, as well as its clients, to the highest standards of privacy. Before handling data from our customers, we carefully weigh relevant factors before deciding to do so. If it is suspected, beyond reasonable doubt, that one of our partners or clients is actively participating in activities that are illegal under privacy laws or regulations, Oddity can and will terminate its participation with the client or partner.

Oddity's product can be installed in two different situations: (1) in a testing environment, living lab, demo area or other non-critical non-production context with the aim of testing, validation and improvement, (2) in a real-world production deployment.

In a testing environment (1; see above), the main aim of the data collection process is to monitor alerts generated by Oddity's algorithm(s) (i.e. an "activation"), log and collect technical statistics surrounding the activation including the relevant video footage, compare the log of activations against crime and incidents statistics as provided by third-parties as well as the video footage collected. Based on this data, Oddity's algorithm(s) are improved so that they become more accurate, more performant and are better able to help improve the safety of citizens, employees or otherwise the subjects of camera surveillance. A contract with a third-party concerning a test (pilot) is always signed for a finite duration after which all video footage and personal data collected as part of the test is irreversibly destroyed or, anonymized and stored for demo-purposes. In accordance with Dutch and European law, video footage as part of the full video archive is removed at most 30 days after it was recorded. Activations (video clips that might contain violence according to the algorithms' decision-making process) are kept (until the end of

the contract) so that they can be used to help improve the algorithm. Video footage on which persons are identifiable that is stored longer than legally allowed is anonymized as required.

In a production environment (2; see above), the main aim of the data collection process is to find anomalies (such as violence) and alert (non-robot) security personnel. Oddity-managed hardware and software systems usually operate as add-on with respect to the existing video surveillance technical infrastructure. As such, in these cases, Oddity does not store video footage or personally identifiable information except for the duration necessary during which the system is still processing and analyzing (which is usually less than a few seconds). During this short period, video frames are kept in a intermediate “video buffer” in the system memory. After analysis, the video frames are tossed. A log of activations (including timestamp, confidence, and other relevant technical metrics) are kept but do not contain personally identifiable information. This data can be shared with the customer if requested. Even though Oddity does not store video data on its systems, the customer (who is the controller of the data and ultimately responsible for it) can (and often does) store video footage on their systems. Please note that, even though Oddity carefully vets potential clients, the customer is the rightful owner of the video data. To understand what data is collected, why and for how long, please refer to the privacy policies of the ultimate controller.

With regards to our video footage analysis practice, please note that we do not profile individuals, do not actively identify persons nor do we make automated decision with impact based on our video analysis results. Our customers might use the results of our analysis to make automated decisions, even though we always recommend that they do not. Our product is built as a tool used by existing security personnel and does not aim to replace them, rather, it helps them to take action more quickly.

With regards to any (video or non-video) personal data that Oddity might process and analyze, but of which Oddity is not the ultimate controller, note that, to assert any of the rights listed below (section “Your rights”), you must seek contact with whomever the ultimate controller is. For example, in the case where you want to assert your “right to forget” with regards to video footage that is taken of you by a public organization or private company that is processed by Oddity (in which Oddity is a sub-processor), you must seek contact with the original owner. Oddity cannot (and often is not allowed to) execute such requests.

Security

Security is a key aspect of keeping the data that we have from being used for other purposes, or by other actors than stated in this privacy policy. As such, we take our system and security infrastructure very serious. Oddity holds itself to the highest standards of security to the extend that can reasonably be expected and takes all precautions necessary to establish a secure technical infrastructure that has the lowest possible risk of data theft, data modification of destruction by external actors.

The data (including video data) we collect are stored on secured servers, and is not publicly accessible. Moreover, only a small subset of our employees have the necessary credentials to view or modify this data. We use software to manage video archives and automate the destruction of data beyond its retention period. Next, we take adequate action to prevent access. Furthermore, employees are instructed to never share video footage that contains personally identifiable information before it is anonymized. Employees are not allowed to download any video data that is not anonymized to their personal systems.

In the event a breach does occur, technical personnel is instructed to make damage control and infrastructure defense their utmost priority until the situation is under control. As much as possible, anyone affected by such a breach will be informed of the situation. Our Data Protection Officer will act as representative and main contact if a breach occurs.

Your rights

You have the right to request, correct or remove personal data that we collect (and of which we are the controller; please refer to the ultimate owner of the data if your request concerns a piece of data that we might have processed for one of our clients). You have the right to opt-out of data

collection completely as well as data transferability. You can contact us to request an archive of all information we have collected on you. If you want to correct, remove or transfer your data, you can use the contact form on our website or use one of the options provided in the uppermost section of this document. To verify that you are requesting this data on your own behalf, we ask you to attach a copy of a valid government-issued ID.

If you suspect video data on which you are personally identifiable is part of one of our datasets (through our research and development efforts), you can assert your rights above only if you can specifically point us to the public source (YouTube, LiveLeak, DailyMotion, academic dataset or other public video data source) of the video clip in question. More specifically, please provide the URL on which your video is accessible (as well as a valid government-issued ID). It is not possible nor legal for us to look you up in our datasets without this information, as we would need to deploy large-scale identification systems to figure out if (and where) you are visible in our datasets. Please note that we never identify individual persons visible in the video footage in our datasets.

Oddity holds high standards for security and all your data is properly protected to prevent abuse, data loss, unauthorized access, publication, and alteration. If you think your data is not properly protected, please contact us using the contact form on our website or using one of the option listed above. If you have any complaints, please be aware that, under European law, you are entitled to file your complaint with the relevant privacy authority. In the case of Oddity.ai B.V., contact the Dutch privacy authority, the “Autoriteit Persoonsgegevens (AP)”, using the following link:

https://autoriteitpersoonsgegevens.nl/nl/contact-met-de-autoriteit-persoonsgegevens/tip-ons.

Other

This document is in effect as of January 2020. Any changes are reflected here. Oddity’s website does not collect personal information itself, but third parties (like Google Analytics, YouTube, crisp.chat, and formspree.io) might. In some cases, these third-party script will respond to a “Do Not Track” signal sent by your browser and allow you to opt-out of data collection through these services altogether.