

# Privacy Notice

## 1. Introduction

The Provider constitutes hereby the present Privacy Notice („Notice”). The Notice supplements the General Terms and Conditions („GTC”).

The aim of the Present Notice is to inform the Users of the method of the data management and of any other facts related to data management, and to ensure the enforcement of the constitutional principles of data management and of the data protection conditions, and to prevent any unlawful amendment, publication or Providerage of and access to the User’s data. This privacy notice aims to inform User about the collection, storage, Providerage and disclosure information about User when User:

- interacts or uses Provider’s websites, including downloading materials from Provider’s resources page (collectively the “websites”),
- if User uses any of Providers products, services or applications (including any trial) (collectively the “Services”) in any manner.

## 2. Applicable laws and Definitions

As a Legal entity established in Malta, EU, the main privacy laws that are applicable to Provider in so far as Users are concerned, are as follows:

- The Maltese Data Protection Act (Chapter 440 of the Laws of Malta) as well as the various subsidiary legislation issued under the same - the ‘DPA’;
- The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) - the ‘GDPR’.

All the above referred to together as the "Data Protection Laws"

User:

The legal provisions regulating the protection of the natural person Users' data refer only to natural person Users as personal data are to be interpreted only regarding natural person. Without reference to the above written, present Notice contains regulation regarding non natural person Users.

Personal data:

Any data of defined (identified or identifiable) natural person relating to the data subject, in particular by reference to the name and identification number of the data subject or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject.

Data management:

any operation or the totality of operations performed on the data, irrespective of the procedure applied; in particular, collecting, recording, registering, classifying, storing, modifying, Providing, querying, transferring, disclosing, synchronizing or connecting, blocking, deleting and destructing the data, as well as preventing their further use, taking photos, making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples, iris scans).

Data manager:

natural or legal person, or organization without legal personality which alone or jointly with others determines the purposes and means of the processing of data; makes and executes decisions concerning data processing (including the means used) or have it executed by a data processor.

Data process:

performing technical tasks in connection with data processing operations, irrespective of the method and means used for executing the operations, as well as the place of execution, provided that the technical task is performed on the data.

Data processor:

any natural or legal person or organization without legal personality processing the data on the grounds of a contract, including contracts concluded pursuant to legislative provisions.

Data transfer:

ensuring access to the data for a third party.

Disclosure:

ensuring open access to the data.

Data deletion:

making data unrecognizable in a way that it can never again be restored.

### 3. The scope of personal data managed by Provider, the aim of data management

The Provider manages data to identify User and other data necessary to provide services. Provider gathers various types of information, including information that identifies or may identify User as an individual (“Personal Information”) as explained in more detail below.

Information User Provides to Provider

From websites:

Provider may collect any Personal Information that User choose to send to Provider or provide to Provider. If User contacts Provider through the websites, Provider will keep a record of the correspondence.

From the Services: Provider receives and stores information User provide directly to Provider. For example, when setting up new Users, Provider collects Personal Information, such as name and email address, to provide them with Services. The types of information Provider may collect directly from Users include: names, Usernames, email addresses, postal addresses, phone numbers, job titles, transactional information

(including Services purchased), as well as any other contact or other information they choose to provide or upload to Provider's systems in connection with the Services.

#### Information Provider Automatically Collects

When User use the websites: When User visits the websites, Provider collects certain information related to User's device, such as User's device's IP address, referring website, what pages User's device visited, and the time that User's device visited the websites.

#### When User uses the Services

- usage information – Provider keeps track of User's activity in relation to the types of Services Users use, the configuration of their computers, and performance metrics related to their use of the Services.
- Log information – Provider log information about Users when uses one of the Services including Internet Protocol ("IP") address.
- Information collected by cookies and other similar technologies – Provider uses various technologies to collect information which may include saving cookies to Users' computers.

For further information, please read the section below headed "Cookies and other Tracking Technologies" and/or read our Cookie Notice.

#### How do Provider uses the information?

##### Provider will use the information collected

- To administer website, events (e.g. sending User event details and updates) and for internal operations, including troubleshooting, data analysis, testing, statistical and survey purposes;
- To improve website to ensure that content is presented in the most effective manner for User and for User's computer;
- For trend monitoring, marketing and advertising;
- For purposes made clear to User at the time User submit User's information;
- As part of Provider's efforts to keep websites secure.

The usage of User's Personal Information may be based on legitimate interest to ensure network and information security, and for direct marketing purposes, or User consenting to it (e.g. when User request a demo). For Users, the use of personal data will be based on the contract Provider have in place.

## Services

Provider may use the information collected from Users in connection with the Services provided for a range of reasons, including to:

- To set up a User account,
- Provide, operate and maintain the Services;
- Process and complete transactions, and send related information, including transaction confirmations and invoices;
- Manage User's use of the Services, respond to enquiries and comments and provide User service and support;
- Send User technical alerts, updates, security notifications, and administrative communications;
- Investigate and prevent fraudulent activities, unauthorized access to the Services, and other illegal activities; and
- For any other purposes about which Provider notify Users.
- Provider uses User's Personal Information in this context based on the agreement that Provider has in place with User. Personal Information will be deleted based on the agreement.

Based on the data management enabled by the laws listed in Section 2. herein the Provider managed the following Users' data (sorted by scopes of purposes):

### 3.1 Billing and collecting fees, and following up Agreements of Users:

- A. name, billing address, phone number of User;
- B. company registration number or other registration number, VAT ID;
- C. date of Service;
- D. payment method;
- E. data regarding payment;

3.2 Following data of User and data needed and necessary to identify User to conclude, word, amend the Service Agreement, and follow up the performance, issue bills on fees and enforce claims according to and arising from the Service Agreement:

- A. notification address, telephone, and e-mail of User;
- B. labeling the Agreement;
- C. short description of User's Complaint and the subject of Fee Complaint;
- D. date and hour of Complaint;
- E. result of investigation the Complaint;
- F. method and date with hour of remedy to the Complaint, provisions fulfilled regarding the fee complaint;
- G. the way and time of informing User.

3.3 With prior and explicit approval of User Provider is entitled to process data listed in Section 4.1 for marketing purposes, and in order to provide value added services in the extend and period of time to provide and sales of the Service in order to inform User about the contracted services (planned amendments and improvements, discounts, new services, promotions, etc.).

3.4 With explicit approval or request of User the Provider is entitled to manage any other personal data of User that make easier to contact or command services (telephone, fax, ID and passport number, e-mail, etc.)

## 4. Method of Data management

User makes declaration regarding the management of his or her data in the course of registration.

While concluding the Service Agreement, User shall be explicit and definitely informed:

- A. that Provider manages his / her personal data;

- B. in which cases and to whom is Provider entitled to transfer data and what decisions is Provider to make in this regard;
- C. what kind of remedy has the User;
- D. about the data management according to Section 3.1;

The User shall be informed immediately about changes in circumstances set in Subsections b)-d).

Provider is entitled to use data of User during the period of time according to the general rules. In case Provider refuses to conclude an Agreement with User, the Provider deletes data of its registry, except for the case User declared otherwise.

Provider deletes all personal data managed otherwise than set in Section 4 immediately as of becoming aware of this fact.

It is prohibited to make the Services available to User only if he / she allows to manage his / her data for an other purpose set in Section 4.

User's data can be utilized for direct marketing, science, survey, market, and statistic research in case the User's explicit subscription.

It is prohibited to transfer any consignment for direct marketing, coverage, survey or market research purposes even with the consent of User, if the identification data of sender are not to recognizable.

A decision which is based solely on automated process of data intended to evaluate certain personal characteristics relating to the data subject shall be permitted only if:

- A. it is taken in the course of the entering into or performance of a contract, provided that the request for entering into or performance of the contract was lodged by the data subject, or
- B. authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

## 5. Period

5.1 In connection with decisions adopted by means of automated data-process systems, the data subject shall, at his request, be informed of the method that is used and its essence, and shall be given the opportunity to express his opinion.

Provider manages and stores all personal data with reasonable diligence. Provider is not responsible in case of damages caused by unpreventable attack if showing reasonable diligence.

5.2 Provider manages data until the end of the term to initiate judicial remedy process or till the legally binding final decision thereon, and until the end of the limitation term of the statistical information providing obligation according to the laws.

5.3 Data managed according to the consent of User can be managed until the amendment or withdrawal of the permission.

5.4 Personal data shall be erased if the purpose of processing no longer exists or the legal time limit for storage has expired.

## 6. Transfer of personal data

Personal data managed by Provider can be transferred or united with other data management process, if the conditions of data management meet in the course of data transfer and united data management process regarding all personal data.

Provider do not rent or sell User's Personal Information to anyone. Provider may share and disclose information (including Personal Information) about Users in the following limited circumstances:

### 6.1 Data transfer to third parties

Vendors, consultants and other service providers:

Provider may share User's information with third party vendors, consultants and other service providers who Provider employ to perform tasks on our behalf. These companies include (for example) our payment processing providers, website analytics

companies (e.g., Google Analytics), product feedback or help desk software providers (e.g. Zoho), CRM service providers (e.g., Zoho), email service providers (e.g., Google) and others. If Provider receives User's Personal Information in the United States and subsequently transfers that information to a third party agent or service provider for processing, Provider remains responsible for ensuring that such third party agent or service provider processes User's Personal Information to the standard required by Provider's Privacy Shield commitments (see the sections below headed "Additional Information for Users in the European Economic Area ("EEA")" and "International Data Transfers").

#### Business Transfers

Provider may choose to buy or sell assets, and may share and/or transfer User information in connection with the evaluation of and entry into such transactions. Also, if Provider (or our assets) are acquired, or if Provider goes out of business, enter bankruptcy, or go through some other change of control, Personal Information could be one of the assets transferred to or acquired by a third party.

#### Group Companies:

Provider may also share User's personal data with Provider's parent companies, subsidiaries and/or affiliates for purposes consistent with this Privacy Notice. Protection of ViddoPro and Others: Provider reserves the right to access, read, preserve, and disclose any information as necessary to comply with law or court order; enforce or apply our agreements with User and other agreements; or protect the rights, property, or safety of ViddoPro, employees, Users, or others. User gives his / her consent by registering that the Provider may transfer his / her personal data to process to a joint venture or contracted partner, subsidiary seated in any EET state or in any third country which fulfills the standard conditions set by the EU regarding the contribution of the provided service.

In the course of present Notice joint ventures are all bProvideriness organizations that control Provider directly or indirectly or the owner of which is partly or fully identical to Provider's owner.

#### 6.2 Transfer of the User's personal data to any other country

#### International Data Transfers

Personal Information User submit on the websites or through the Services is sent to the United States and will be primarily processed by Provider in the United States and potentially in other countries, on our servers or on our hosted service providers' cloud servers on our behalf. These countries may not have similar data protection laws to those in User's country of residence. However, Provider will always protect User's information in accordance with this Privacy Notice wherever it is processed. Some of Provider's product offerings include the ability to host User's data in servers located in the EU or other countries. To request this capability, contact [support@viddo.com](mailto:support@viddo.com).

International Data Transfers - Additional information for Users in the European Economic Area ("EEA")

Self-certified to the EU-Provider Privacy Shield Framework

This section sets out the privacy principles Provider follow with respect to transfers of Personal Information from the EEA to the United States, including Personal Information Provider receive from individuals residing in the EEA who visits our websites and/or who may use of our Services or otherwise interact with Provider. Please note that for Users located in the EEA, the term Personal Information used in this notice is equivalent to the term "personal data" under applicable European data protection laws. Provider comply with the EU-U.S. Privacy Shield Framework ("Privacy Shield") as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Information from European Union member countries. Provider have certified that Provider adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability. If there is any conflict between the policies in this Privacy Notice and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, see the Provider Department of Commerce's Privacy Shield website located at <https://www.privacyshield.gov>. To view our certification on the Privacy Shield list, please visit <https://www.privacyshield.gov/>

In compliance with the EU-U.S. Privacy Shield Principles, Provider commits to resolve complaints about User's privacy and our collection or use of User's Personal Information. Individuals located within the EEA with inquiries or complaints regarding this Privacy Notice should first contact ViddoPro at: [support@viddo.com](mailto:support@viddo.com)

Provider will investigate and attempt to resolve any complaints or disputes regarding the use or disclosure of personal data within 45 days of receiving User's complaint. Provider have further committed to refer unresolved privacy complaints under the EU-U.S. Privacy Shield Principles BBB EU PRIVACY SHIELD, a non-profit alternative dispute resolution provider located in the United States and operated by the Council

of Better Business Bureaus. If User do not receive timely acknowledgment of User's complaint, or if User's complaint is not satisfactorily addressed, please visit [www.bbb.org/EU-privacy-shield/for-eu-consumers/](http://www.bbb.org/EU-privacy-shield/for-eu-consumers/) for more information and to file a complaint. Under certain limited circumstances, individuals in the EEA may invoke binding Privacy Shield arbitration as a last resort if all other forms of dispute resolution (discussed above) have been unsuccessful. To learn more about this method of resolution and its availability to User, please visit <https://www.privacyshield.gov/>. Provider are subject to the jurisdiction of the U.S. Federal Trade Commission for purposes of Privacy Shield enforcement. Please note that ViddoPro is required to disclose Personal Information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

#### Self-certified to the Swiss-U.S. Privacy Shield Framework

Provider comply with the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from Switzerland to the United States. Provider have certified to the Department of Commerce that Provider adhere to the Privacy Shield Principles. If there is any conflict between the terms in this Privacy Notice and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit <https://www.privacyshield.gov/>. In compliance with the Swiss-Provider Privacy Shield Principles, Provider commit to resolve complaints about User's privacy and our collection or use of User's personal information. Swiss individuals with inquiries or complaints regarding this Privacy Notice should first contact ViddoPro at: [support@viddo.com](mailto:support@viddo.com)

Provider has further committed to refer unresolved privacy complaints under the Swiss-Provider Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by the Council of Better Business Bureaus. If User do not receive timely acknowledgment of User's complaint, or if User's complaint is not satisfactorily addressed, please visit <http://www.bbb.org/EU-privacy-shield/for-eu-consumers> for more information and to file a complaint. Under certain limited circumstances, individuals in Switzerland may invoke binding Privacy Shield arbitration as a last resort if all other forms of dispute resolution (discussed above) have been unsuccessful. To learn more about this method of resolution and its availability to User, please visit <https://www.privacyshield.gov/>.

#### California and Delaware "Do Not Track" Disclosures

California and Delaware law require ViddoPro to indicate whether it honors “Do Not Track” settings in User's browser concerning targeted advertising. ViddoPro adheres to the standards set out in this Privacy Notice and does not monitor or respond to Do Not Track browser requests.

### Children

Provider do not knowingly collect or solicit personal information from anyone under the age of 16. If User are under 16, please do not attempt to register for the Services or send any Personal Information about themselves to Provider. If Provider learns that Provider has collected Personal Information from a child under age 16, Provider will delete that information as quickly as possible. If User believe that a child under 16 may have provided Provider Personal Information, please contact Provider at [support@viddo.com](mailto:support@viddo.com)

### Linked websites

For User's convenience, hyperlinks may be posted on the websites that link to other websites (the “Linked Sites”). Provider is not responsible for, and this Privacy Notice does not apply to, the privacy practices of any Linked Sites or of any companies that Provider do not own or control. Linked Sites may collect information in addition to that which Provider collects on the websites. Provider does not endorse any of these Linked Sites, the services or products described or offered on such Linked Sites, or any of the content contained on the Linked Sites. Provider encourages User to seek out and read the privacy notice of each Linked Site that User visit to understand how the information that is collected about User is used and protected.

User gives his / her consent with the registration to Provider to transfer User's data to other data manager in the territory of EU for scientific, and survey or market research purposes.

Transfer of data to EEA Member States shall be considered as if the transmission took place within the territory of Malta.

According to present Notice EET member state are all member states of EU and all other states contracted in the Agreement on the European Economic Area, furthermore states whose citizens are to be considered as citizens of states contracted in the Agreement on the European Economic Area based upon international agreement between the EU, EU member states and the state not contracted in the Agreement on the European Economic Area.

User is entitled to make any declaration regarding his / her personal data managed in a third country on his / her mother language and to request for information regarding the joint ventures, contacted partners and personal data managed or processed thereby.

Provider declares not to transfer any personal data whatsoever to third countries which does not fulfill the standard conditions set by the EU.

6.3 Transfer according to laws, disclosures for National Security or Law Enforcement:

Under certain circumstances, Provider may be required to disclose User's Personal Information in response to valid requests by public authorities, including to meet national security or law enforcement requirements.

Third parties receiving Users' data are bound to protect and keep data confidential with the same conditions as Provider.

## 7. Obligations of Provider

The Provider is obliged to provide the security of Users' personal data, and to organize the data management operation so that the private sphere of all related parties are secured while applying the effective laws, and any other regulation on data management.

Employees, partners, subcontractors and assignees of Provider are obliged to fulfill the same conditions as Provider regarding the data protection and confidence.

Provider is obliged to fulfill the following conditions regarding the tasks set above:

Mirroring: To prevent the destruction of data on the server, data have to be mirrored to a physically different data storage.

Archiving: The passive part of the databases containing personal data have to be separated from the active parts of it, then the passive data have to be recorded.

Fire protection: Data and databases have to be placed in a room with fire and property protection equipments.

Virus protection: the PC's of clerks, employees managing personal data have to be exempted from viruses.

Access protection: only with personalized and valid, identifiable entitlement is the access to data available. Network resources are available only with valid email address and password.

Network protection: By using IT equipments available at all times all access of any unauthorized person has to be prevented to the servers accessible through the network containing data.

Provider use appropriate technical, organizational and administrative security measures to protect any information Provider hold in our records from loss, misuse, and unauthorized access, disclosure, alteration and destruction.

By using Zoho Provider informs the Users on the above certificated security conditions:

#### ISO/IEC 27001:2013 Certified

Our Information Security Management System (ISMS) is ISO/IEC 27001:2013 certified as reflected in the certificate found here: The audit established the overall operational effectiveness of a sample of control areas comprising Zoho's ISMS.

#### SOC 2

Zoho has been audited and received a SOC 2 report addressing the security, confidentiality and availability of our services. Unfortunately, no company or service can guarantee complete security. Unauthorized entry or use, hardware or software failure, and other factors, may compromise the security of User information at any time. Among other practices, User's account is protected by a password for User's privacy and security. User must prevent unauthorized access to User's account and Personal Information by selecting and protecting User's password appropriately and limiting access to User's computer or device and browser by signing off after User have finished accessing User's account.

#### How and Why Provider use Cookies and Other Tracking Technologies

A cookie is a small piece of data (text file) that a website – when visited by a User – asks User's browser to store on User's device in order to remember information about

User, such as User's language preference or login information. Those cookies are set by Provider and called first party cookies. Provider also use third party cookies – which are cookies from a domain different than the domain of the website User are visiting – for our advertising and marketing efforts. More specifically, Provider use cookies and other tracking technologies for the following purposes:

- Assisting User in navigation;
- Assisting in registration to our events, login, and User's ability to provide feedback;
- Analyzing User's use of our products, services or applications;
- Assisting with our promotional and marketing efforts (including behavioral advertising).

Below is a detailed list of the cookies Provider use on our website. Our website is scanned with our cookie scanning tool regularly to maintain a list as accurate as possible. Provider classify cookies in the following categories:

- Strictly Necessary Cookies
- Performance Cookies
- Functional Cookies
- Targeting Cookies

User can opt-out of each cookie category (except strictly necessary cookies) by clicking on the “cookie settings” button at the bottom of the page or in our Cookie Notice.

#### Google Analytics:

Provider also utilize Google Analytics, a web analysis service provided by Google, to better understand User's use of our websites and Services. Google Analytics collects information such as how often Users visit the websites, what pages they visit and what other sites they used prior to visiting. Google uses the data collected to track and examine the use of the websites, to prepare reports on its activities and share them with other Google services. Google may use the data collected on the websites to contextualize and personalize the ads of its own advertising network. Google's ability to use and share information collected by Google Analytics about User's visits to the websites is restricted by the Google Analytics Terms of use and the Google Privacy Notice. Google offers an opt-out mechanism for the web available here. Please consult our Cookie Notice for more information about the type of cookies and tracking technologies that Provider use on this website and why, and how to accept and reject them.

Further information about Google's privacy policy may be obtained from this link.

Be assured that neither Google nor Provider will ever use this information to identify individual Users or to match it with further data on an individual user.

If User does not wish that User's behaviour is analysed, User can opt-out of this service respectively via the following link - [Google Analytics Opt-Out](#).

## 8. Rights of User

User can always opt not to disclose information to Provider, but keep in mind some information may be needed to register with Provider or to take advantage of some of our features.

### Cookies

User can accept or reject cookies accessible by clicking the "cookie settings" button in our Cookie Notice. User can also do so by adjusting User's web browser controls. Please consult the Cookie Notice for more information about Provider's use of cookies and how to accept and reject them.

### Marketing Communications

User can opt-out of receiving certain promotional or marketing communications from Provider at any time, by using the unsubscribe link in the emails communications Provider send by Zoho Campaign, CRM or Sendgrid. If User have any account for Provider's Services, Provider will still send User non-promotional communications, like service related emails.

If User would like to access, review, update, rectify, and delete any Personal Information Provider holds about User, or exercise any other data subject right available to User under the EU General Data Protection Regulation (GDPR), User can either click the the User profile at the User's dashboard, and choose Delete my account button to move forward with the procedure. To protect User's interest the delete option will not be available until there is an active voucher under User's registration. Please note that Provider may still use any aggregated and de-identified Personal Information that does not identify any individual, and may also retain and use User's information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. California residents are entitled to ask Provider for a notice identifying the categories of Personal Information which Provider share with our affiliates and/or third parties for marketing purposes, and providing contact information for such affiliates and/or third parties. If User are a California resident and would like a copy of this notice, please submit a written request to:

support@viddo.com If User are a resident of the European Economic Area, please see the section below headed “Additional Information for Users in the European Economic Area” for further information about User's privacy rights.

The User is entitled to request

- A. information on his personal data being processed,
- B. the rectification of his personal data, and
- C. erasure or restriction of processing of his personal data, except for cases of compulsory data management.
- D. Data portability to other data controllers, where technically feasible

Furthermore User is entitled to:

- A. Object to the processing of his / her personal data];
- B. get Judicial remedy;
- C. Amend, withdraw his / her consent regarding data management.

If User considers that Provider's processing of User's personal information infringes data protection laws, User can contact us on support@viddo.com or via our website. User also has a legal right to lodge a complaint with a supervisory authority responsible for data protection. In Malta the supervisory authority is the Information and Data Protection Commissioner.

### 8.1 Request for information

Upon the data subject's request the Provider shall provide information concerning the data relating to him, including those processed by a data processor on its behalf or according to his/her notice, the sources from where they were obtained, the purpose, grounds and duration of processing, the name and address of the data processor and on its activities relating to data processing, and the conditions and effects of the data incident and measures taken with a view to eliminate them and -in case of data transfer - the legal basis and the recipients.

Providers must comply with requests for information without any delay, and provide the information requested in an intelligible form, in writing at the data subject's request, within not more than thirty days.

### 8.2 Request for correction

Where a personal data is deemed inaccurate, and the correct personal data is at the Provider's disposal, the Provider shall rectify the personal data in question.

### 8.3 Erasure or restriction of Data

#### Right to Erasure (The Right to be Forgotten)

User has the right to ask Provider to delete his / her Personal Data and Provider shall comply without undue delay but only where:

- The Personal Data is no longer necessary for the purposes for which it was collected; or
- User has withdrawn his / her consent (in those instances where Provider processes on the basis of User's consent) and Provider has no other legal ground to process Users Personal Data; or
- User shall have successfully exercised his / her right to object (as explained below); or
- User's Personal Data shall have been processed unlawfully; or
- There exists a legal obligation to which Provider is subject; or
- Special circumstances exist in connection with certain children's rights.

In any case, Provider shall not be legally bound to comply with User's erasure request if the processing of User's Personal Data is necessary:

- For exercising the right of freedom of expression and information; or
- For compliance with a legal obligation to which Provider is subject (including but not limited to Provider's data retention obligations); or
- For the performance of a task carried out in the public interest; or
- For the performance of a task carried out in the exercise of official authority vested in Provider; or
- For reasons of public interest in the area of public health; or
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (under certain conditions); or
- For the establishment, exercise or defence of legal claims.

#### User's Right to Data Restriction

User has the right to ask Provider to restrict (that is, store but not further process) User's Personal Data but only where:

- The accuracy of User's Personal Data is contested (see the right to data rectification above), for a period enabling Provider to verify the accuracy of the Personal Data; or
- The processing is unlawful and User oppose the erasure of User's Personal Data; or
- Provider no longer need the Personal Data for the purposes for which they were collected but User need the Personal Data for the establishment, exercise or defence of legal claims; or
- You exercised User's right to object and verification of Provider's legitimate grounds to override Your objection is pending.

Following User's request for restriction, except for storing User's Personal Data, Provider may only process User's Personal Data:

- Where Provider has User's consent; or
- For the establishment, exercise or defence of legal claims; or
- For the protection of the rights of another natural or legal person; or
- For reasons of important public interest.

#### 8.4 The User's right to protest against the processing of his / her personal data

The User has the right to object to the processing the personal data related to him / her,

- A. If processing or disclosure is carried out solely for the purpose of discharging the Provider's legal obligation or for enforcing the rights and legitimate interests of the Provider, the recipient or a third party, unless processing is mandatory;
- B. if personal data is used or disclosed for the purposes of direct marketing, public opinion polling or scientific research; and
- C. in all other cases prescribed by law.

In the event of objection, the Provider shall investigate the cause of objection within the shortest possible time inside a fifteen-day time period, adopt a decision as to merits and shall notify the data subject in writing of its decision.

If, according to the findings of the Provider, the data subject's objection is justified, the Provider shall terminate all processing operations (including data collection and transmission), block the data involved and notify all recipients to whom any of these data had previously been transferred concerning the objection and the ensuing measures, upon which these recipients shall also take measures regarding the enforcement of the protest.

The Provider shall not delete the data of the data subject if processing has been prescribed by law.

However, data may not be disclosed to the data recipient if the Provider agrees with the objection or if the court has found the objection justified.

#### 8.5 Judicial remedy

In case of breaching his / her rights User is entitled ask for judicial remedy.

The independent and only to the laws subordinated Authority set up to protect the fundamental right of protection of personal data according to GDPR shall be responsible to supervise and promote the enforcement of the rights to the protection of personal data and access to public information and information of public interest

Any person shall have the right to notify the Authority and request an investigation alleging an infringement relating to his or her personal data or concerning the exercise of the rights to access to public information or information of public interest, or if there is imminent danger of such infringement.

## 9. Change to the Privacy Notice and Contact Provider

Provider is constantly trying to improve our websites and Services, so Provider may need to change this Privacy Notice from time to time as well. Provider will alert User to material changes by, for example, placing a notice on our websites and/or by

sending User an email (if User have registered User's e-mail details with Provider) when Provider are required to do so by applicable law. User can see when this Privacy Notice was last updated by checking the date at the top of this page. Users are responsible for periodically reviewing this Privacy Notice.

ViddoPro is a trademark of [VIS Kft.] which is the party in interest herein ViddoPro [VIDDO Limited, Central Business Centre, Room 1, Level 1, Suite 2, Mdina Road, Zebbug ZBG 9015, Malta]

If User have any questions or concerns regarding our privacy notice, please send a detailed message to [support@viddo.com](mailto:support@viddo.com) or by mail to the address listed above.