Version: 1.0 Updated: 17 April 2018

Data protection policy

1 INTRODUCTION

ObjectPlanet AS needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

ObjectPlanet AS is committed to safeguarding personal data of our website visitors and users of our applications and services. This policy is applicable in situations where we are acting as data controller or data processor with respect to this personal data. According to the EU regulation on General Data Protection (May 25. 2018), the “data controller” is the entity that determines the purpose and means of processing this personal data. The “data processor” is the entity that in some way handles the data on under the instructions of the data controller. In our case we will act as data controller for our internal systems where we store personal data needed for maintaining normal customer relationships. We act as processor when our customers use our services to store their data.

This policy describes how this personal data must be collected, handled and stored to meet our data protection standards and to comply with the law.

In this document, "we", "us" and "our" refer to *ObjectPlanet AS*.

To contact us regarding this policy:

ObjectPlanet AS
Øvre Slottsgate 5
0157 Oslo
Norway

Phone: +47 2233 3360
Electronically: http://www.objectplanet.com/GDPR.html

2 GOAL OF THE DATA PROTECTION POLICY

The goal of the data protection policy is to depict the legal data protection aspects in one summarizing document. This is not only to ensure compliance with the European General Data Protection Regulation (GDPR) but also to provide proof of compliance.

This data protection policy ensures ObjectPlanet AS:

- complies with data protection law and follow good practice
- protects the right of staff, customers and partners
- is open about how it stores and processes individuals’ data
- protects itself from the risks of data breach

3 PERSONAL DATA WE COLLECT AND HOW IT IS USED

Below are the kinds of data we collect and the reasons for doing so. We do not use this data for other purposes.

- We may collect and process data about the use of our website and services (“usage data”). This data may include browser type and version, length of visit, page views, IP address, number of visits and similar data. This information is needed to understand our website traffic profile and how people are using the website.
- We may process your name, address, email address, phone number, physical address, occupation and similar information (“account data”). This is used for operating our website, providing our services like hosting of applications, support agreements, software development and the like.
- We may collect profile data (“profile data”). The profile data may include name, address, email address, phone number, physical address, occupation and similar information. This is used for operating our website, providing our services like server hosting, support agreements, software development and the like.
- We may process information relating to purchases of goods and services (“transactional data”) that we collect from you through our website. The transactional data may include your contact details, your credit card details and other information needed to complete the transaction. The legal basis for this processing is to facilitate the processing of the transaction, at your request.
- We may collect and process information contained in or related to any communication that you send to us ("correspondence data"). The correspondence data may include name, email address, and any other information included in the correspondence that you send to us. It is necessary to store this information in order to provide you with a quality service (sales inquiries and support).
- Data may be stored in your browser. This is called "cookies", and usually contains a string of numbers and characters to identify your browser and track your movements around our website and applications. The cookies are also necessary to maintain a session where authentication is required. We may also use Google analytics to analyze and understand web traffic on our website, which also stores cookies in your browser. Our website will ask for your consent regarding the use of cookies in your browser. Google's privacy policy is available at: https://www.google.com/policies/privacy/
- We may process data that is collected by our clients when using our services. We are hosting our survey software, Opinio, that provides the functionality to collect data from survey respondents about their personal data. It is the responsibility of the data controller (our clients who publish the surveys) to make sure their data protection measures are compliant with the law. It is our responsibility as processor that we have the appropriate security measures in place.

4 LEGAL BASIS FOR PROCESSING YOUR DATA

We may process any of your personal data where such processing is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

Please do not supply any other person’s personal data to us, unless we prompt you to do so.

The legal basis for this processing of personal information is:

- consent, or
- it may be in our legitimate interests, namely the maintenance of our website and business, or
- the preparation and execution of a contract between you and us.

5 ROLES AND RESPONSIBILITIES

Depending on the data and how it is used, several people may be involved processing the personal data.

The roles and responsibilities for protecting your data are:

- the board of directors is ultimately responsible for ensuring that ObjectPlanet AS meets its legal obligations.
- GDPR contact, Torgeir Lund, is responsible for:
    - keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with the requests from individuals to see the data ObjectPlanet AS holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The IT manager, Eivind Pedersen, is responsible for:
    - ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third party services the company is considering using to store or process data.
- General staff is responsible for:
    - the only people able to access data covered by this policy should be those who need it for their work.
    - Data should not be shared informally. When access to confidential information is required, employees can requested from their line managers.
    - ObjectPlanet AS Will provide training to all employees to help them understand their responsibilities when handling data.
    - Employees should keep all data is secure, by taking sensible precautions and following the guidelines below.
    - In particular, strong passwords must be used and they should never be shared.
    - Personal data should not be disclosed to unauthorized people, either within the company or externally.
    - Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
    - Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

6 DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is stored electronically:

- data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be cited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

When data is stored on paper:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and print outs are not left where unauthorized people could see them, like on a printer.
- Data print outs should be shredded and disposed of securely when no longer required.

7 DATA USE

Personal data is of no value to us unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of calm indication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to unauthorized external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update central copy of any data.

8 DATA ACCURACY

It is the responsibility of all employees who work with the data to take reasonable steps to ensure it is kept is accurate and up-to-date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- ObjectPlanet AS will make it easy for data subjects to update the information ObjectPlanet AS holds about them. For instance, via the company website.
- Data should be updated as in accuracies are discovered. For instance if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

9 ACCESS YOUR DATA – CONTACT US

All individuals who are the subject of personal data held by ObjectPlanet AS are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up-to-date.
- Be informed how the companies meeting its data protection obligations.
- Request removal

If contact us regarding this information, it is called a "subject access request."

Subject access requests from individuals should be requested at this web address:
http://www.objectplanet.com/GDPR.html

By sending a request through this form, the special GDPR contact will be notified and will handle your case.

A subject access request is in most cases free, but we may require a 15 USD payment if the request is unreasonably detailed or is a repeated request. The data controller will always verify the identity of anyone making a subject access request before handling over any information.

10 COMPLAINTS

You are entitled to file complaints to the supervisory authorities that oversees the regulations for personal data protection within the EU/EEA. In Norway, the contact information is:

Datatilsynet
P.O. Box 8177 Dep.
NO-0034 Oslo
Norway

Email: postkasse@datatilsynet.no
Phone: + 47 22 39 69 00

11 Disclosing personal data

Your personal data will not be shared with other parties, except where your explicit consent is given to us.

Under certain circumstances, the data protection act allows your personal data to be disclosed to law enforcement agencies without your consent.

Under these circumstances, ObjectPlanet AS will disclose requested data. However, we will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisors where necessary.

12 Data retention

Personal data will be deleted when

- the data is no longer needed by us to provide our products and services
- the data is requested to be deleted by you

In certain cases, we are required by law to retain some information for a period of time (recordkeeping and accounting for the most part). This will take precedence when deciding to delete the information or not.

13 Data stored outside the EU

We are located in Oslo, Norway. Norway is not part of the EU, but is conforming to the EU rules on personal data protection through the European Economic Area (EEA) in which Norway is a member. We will do all we can to make sure your personal data is stored within the EU or EEA. The servers used to store your data will be located in Norway or another EU country.

14 Amendments

We may update this policy from time to time by publishing a new version on our website.

You should check this page occasionally to ensure you are happy with any changes to this policy. We may notify you of changes to this policy by email.

You can find the latest version of this document here:

http://www.objectplanet.com/DataProtectionPolicy-ObjectPlanet.pdf

A shorter address, to make it easy to type in your browser (case sensitive):
bit.ly/2qEYAis