Updating Netsight's License Agreement and Privacy Policy for GDPR

The GDPR is a data protection law from the European Union that gives you more transparency and control over how your personal data is dealt with. It is applicable to any organisation that processes personal data of European Union individuals, regardless of where the organisation is based.

Similar to many SaaS providers, we use a top-tier, third-party data hosting provider (Amazon Web Services) to host our online and mobile services. Servers are housed in EU approved locations when applicable. For more information about AWS's approach to compliance with the GDPR, see https://aws.amazon.com/compliance/gdpr-center/

Under the GDPR, where an organisation ("processor") processes personal data on behalf of another organisation which determines the purposes and means by which that data is processed ("controller"), there must be a written agreement in place between the controller and processor containing certain minimum provisions. In using Netsight, our customers are controllers and Netsight is a processor of the personal data that we receive. This mainly comprises information relating to your employees that use myosh (eg name, email address) and also personal data that your employees may collect on other individuals for the purposes of managing Workplace Health and Safety using mobile devices and web browsers.

Summary of Updates to our License Agreement

- There is a new Clause (Data Protection) which introduces, to the extent that the GDPR is relevant to you, Appendix A and B;
- Appendix A contains data protection compliance definitions and provisions, including stating that you, as a controller, will comply with your obligations under GDPR, and we will comply with the provisions set out in Appendix B;
- Appendix B is the Data Processing Agreement, and contains the substance of the changes, setting out our obligations, such as:
    1. only to process personal data based on your instructions;
    2. to implement appropriate data security;
    3. to assist you with complying with requests from data subjects to exercise their rights;
    4. to assist you in complying with data security, breach notification and impact assessment obligations;
    5. cooperating with compliance audits; and
    6. deleting or returning personal data at the end of the contract.

The following clause been added to our licence agreements:

Data Protection Clause

This Section shall only apply if and to the extent that the EU General Data Protection Regulation 2016/679 ("GDPR") applies to any of the data with which you use the Service. If this Section applies, the provisions of Appendix A (Data Protection Compliance) and Appendix B (Data Processing Agreement) shall apply.

Appendix A and Appendix B have been added to our license agreements

Appendix A (Data Protection Compliance)
In this Appendix and in Appendix B (Data Processing Agreement):

Data Protection Laws means the EU Data Protection Laws and the laws of other states and territories that create and regulate substantially similar concepts and legal principles as are contained in the EU Data Protection Laws in relation to the processing of personal data and sensitive personal data.

EU Data Protection Laws means, up to and including 24 May 2018, any legislation in force from time to time which implements the EU Directive 95/46/EC and relevant national implementations of the same and, with effect on and from 25 May 2018, means the GDPR and any relevant national implementations of the same;

Personal Data, **Sensitive Personal Data**, **Consent**, **Controller**, **Processor**, **Data Subject** and P**rocessing** mean those concepts, roles and activities as defined in the applicable EU Data Protection Laws and on and from 25 May 2018 sensitive personal data means those classes of personal data that are described in Article 9 of the European General Data Protection Regulation 2016/679) or, where relevant, equivalent concepts, roles and activities as described in other Data Protection Laws.

We are the controller in respect of personal data and sensitive personal data, such as account registration details, that we collect directly from users of the Services (**End Users**) and which we use for the purposes of our business.

You are the controller and we are the processor in respect of any other personal data and sensitive personal data (including within Your Customisations) that is uploaded by End Users including data, templates, information, content, code, video, images or other material of any type (Materials)

On and from 25 May 2018, to the extent that the Services comprise the processing of personal data or sensitive personal data where we are the processor and you are the controller and the processing of personal data or sensitive personal data is subject to the GDPR:

- you will comply with the requirements of the GDPR as the same apply to you as controller of the personal data or sensitive personal data; and

- the provisions of Appendix B (Data Processing Agreement) to these Terms shall apply

We will make our Privacy Policy available to you through our web site and to others who may use the system. To the extent that we do not have direct contact with End Users or the relevant data subjects, for example, where personal data or sensitive personal data is uploaded relating to your employees or customers, and where we are a processor and not a controller, it is your responsibility to ensure that in accordance with Article 13 of the GDPR:

- There is a lawful basis for the collection and processing of personal data and/or sensitive personal data; and

Appendix B (Data Processing Agreement)

The provisions of this Appendix (Data Processing Agreement) form part of the Agreement to the extent that the Data Protection Clause Applies.

Netsight shall:

1. process personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by European Union or the national law of an EU member state to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
2. ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
3. implement appropriate organisational and technical measures as required pursuant to Article 32 (security of processing) of the EU General Data Protection Regulation 2016/679. The measures that we consider appropriate are more fully described in Netsight's Security document (a copy of which is available on our web site http://www.myosh.com/security/). This document outlines:
    - our architecture and infrastructure through which Services provided;
    - security controls employed by us and our service providers in protecting personal and/or sensitive personal data; and
    - security controls employed by our support team which handle personal data or sensitive personal data.
4. respect the conditions for engaging another processor referred to in paragraphs 2 and 4 of Article 28 (processor) of the EU General Data Protection Regulation 2016/679;
5. taking into account the nature of the processing, assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the EU General Data Protection Regulation 2016/679;
6. assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the EU General Data Protection Regulation 2016/679 taking into account the nature of the processing and the information available to the processor;
7. at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of services relating to processing, and delete existing copies unless EU law or the national law of an EU member state or another applicable law, including any Australian state or Commonwealth law to which the processor is subject requires storage of the personal data;
8. make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 (processor) of the EU General Data Protection Regulation 2016/679 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (in each case at the controller's cost).

Summary of Additions to the Privacy Policy:

- We have introduced a new GDPR Appendix, which applies only to the extent that our processing of your data is covered by GDPR. This Appendix includes provisions such as:
    1. The legal basis for processing your information;
    2. Third party service providers;
    3. Processing outside of the European Economic Area;
    4. Retention of personal data;
    5. Your rights in respect of information we hold about you
    6. Automated decision-making; and
    7. Complaints

Appendix A - GDPR

The Legal Basis for Processing your Information

Under GDPR, the main grounds that we rely upon in order to process personal data collected via our websites and services are the following:

(a) Necessary for entering into, or performing, a contract – in order to perform obligations that we undertake in providing a service to you, or in order to take steps at your request to enter into a contract with us, it will be necessary for us to process your personal data;

(b) Necessary for compliance with a legal obligation – we are subject to certain legal requirements which may require us to process your personal data. We may also be obliged by law to disclose your personal data to a regulatory body or law enforcement agency;

(c) Necessary for the purposes of legitimate interests - either we, or a third party, will need to process your personal data for the purposes of our (or a third party's) legitimate interests, provided we have established that those interests are not overridden by your rights and freedoms, including your right to have your personal data protected. Our legitimate interests include responding to requests and enquiries from you or a third party, optimising our website, applications and customer experience, informing you about our products and services and ensuring that our operations are conducted in an appropriate and efficient manner;

(d) Consent – in some circumstances, we may ask for your consent to process your personal data in a particular way.

Processing Outside of the European Economic Area ("EEA")

To the extent that any personal information is provided to third parties outside the EEA, or who will access the information from outside the EEA, we will ensure that approved safeguards are in place to ensure that we comply with GDPR, such as the standard contractual clauses approved by the European Commission or the EU/US Privacy Shield.

Netsight processes personal information on our servers in Australia and the USA. We may process your personal information on a server located outside the country where you live, including outside the EEA. The primary location of user data and data uploaded to myosh is a datacentre in the U.S. operated by our third-party cloud hosting provider, Amazon Web Services ("AWS"). AWS is a participant in the EU/US Privacy Shield, under which transfers of personal data to the U.S. are authorised.

Retention of Personal Data

We will retain your personal information for the time necessary to provide the services we perform for you, or to achieve other purposes outlined in this Privacy Policy, and you can always request that we stop processing or delete your personal information (see the section below regarding your rights).

Your rights in respect of information we hold about you :

You have certain rights in relation to personal information we hold about you. Details of these rights and how to exercise them are set out below. We will require evidence of your identity before we are able to act on your request.

Right of Access

You have the right at any time to ask us for a copy of the personal information about you that we hold. Where we have good reason, and if the GDPR permits, we can refuse your request for a copy of your personal information, or certain elements of the request. If we refuse your request or any element of it, we will provide you with our reasons for doing so.

Right of Correction or Completion

If personal information we hold about you is not accurate, out of date or incomplete, you have a right to have the data rectified, updated or completed. You can let us know by contacting us at support@myosh.com.

Right of Erasure

Under certain circumstances, you have the right to request that personal information we hold about you is erased e.g. if the information is no longer necessary for the purposes for which it was collected or processed or our processing of the information is based on your consent and there are no other legal grounds on which we may process the information.

Right to object to or restrict processing

In certain circumstances, you have the right to object to our processing of your personal information by contacting us at support@myosh.com. For example, if we are processing your information on the basis of our legitimate interests and there are no compelling legitimate grounds for our processing which override your rights and interests. You also have the right to object to the use of your personal information for direct marketing purposes.
You may also have the right to restrict our use of your personal information, such as in circumstances where you have challenged the accuracy of the information and during the period where we are verifying its accuracy

Right of Data Portability

In certain instances, you have a right to receive any personal information that we hold about you in a structured, commonly used and machine-readable format. You can ask us to transmit that information to you or directly to a third party organisation.

The above right exists only in respect of personal information that:

- you have provided to us previously; and

- is processed insofar as is necessary for the implied purpose of the software

While we are happy for such requests to be made, we are not able to guarantee technical compatibility with a third party organisation's systems. We are also unable to comply with requests that relate to personal information of others without their consent.

You can exercise any of the above rights by contacting us using any of the methods in the Contact section above.

Most of the above rights are subject to limitations and exceptions. We will provide reasons if we are unable to comply with any request for the exercise of your rights.

To the extent that we are processing your personal information based on your consent, you have the right to withdraw your consent at any time. You can do this by contacting us using the details in the Contact section above.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. It is specifically regulated under GDPR where such decisions are taken which have legal or other significant effects on individuals. It is permitted in the following circumstances:

1. Where it is necessary to enter into or perform our contract with you and appropriate measures are in place to safeguard your rights.
2. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated processing, unless we have a lawful basis for doing so, we have notified you and given you a right to challenge the decision or to require that the decision be taken by a person.

Complaints

If you are unhappy about our use of your personal information, you can contact us using the details in the Contact section below. You are also entitled to lodge a complaint with the UK Information Commissioner's Office using any of the below contact methods:
Telephone: 0303 123 11113
Website: https://ico.org.uk/concerns/
Post: Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

If you live or work outside the UK or you have a complaint concerning our activities outside the UK, you may prefer to lodge a complaint with a different supervisory authority. A list of relevant authorities in the EEA and the European Free Trade Area can be accessed here.

Appendix B – Third Party Service Providers (Updated on an ongoing basis)

Third Party Service/ Vendor	Purpose	Entity Country
Zendesk	Ticketing System for support calls	USA
AWS Amazon	Data hosting	USA, Australia
Hub Spot	Customer Relationship Management	USA
Xero	Accounting System	USA
eWAY	Merchant Bankers	AUS

By continuing to use myosh you acknowledge the additions to our Privacy Policy and agree to the additional clause and Appendix A and Appendix B to the myosh License Agreement.

If you have any questions in relation to the changes, please contact us at support@myosh.com .

From
The myosh team