

## Annex A NGS Data Protection Policy 2020

**NGS Privacy Notice (Medical and Non-Medical)**

As the contracted Emergency Response Company, NGS has been contracted by your employer to step in at your request and provide additional resources, crisis management and/or Emergency Response in the event of a crisis or emergency. This privacy notice explains why we're processing and sharing your personal data. At no stage will your information be used for any other purpose than what it was gained for or used in any automated profiling.
<b>Who we are:</b>
Northcott Global Solutions – Emergency Medical and Non-Medical Response Company
<b>Why we need to process your information</b>
As the contracted Emergency Response Company, NGS has been contracted by your employer to step in at your/their request if you need help, emergency response, crisis management in the event of a crisis or emergency and where required, handle any complaints.
<b>Legal basis for processing your information.</b>
<b>Consent</b>
<b>Contract</b> - you need to process someone's personal data to fulfil your contractual obligations to them; or because they have asked you to do something before entering into a contract (e.g. provide a quote).
<b>Legal Obligation</b> - you need to process the personal data to comply with a common law or statutory obligation. You must be able to identify the legal obligation.
<b>Vital Interests</b> - if you need to process the personal data to protect someone's life. You cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.
<b>Legitimate Interests</b> - the most "flexible" lawful basis for processing data. There is a three-part test: a. identify a legitimate interest; b. show that the processing is necessary to achieve it; and c. balance it against the individual's interests, rights and freedoms. If you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing, then this basis works. Keep a record of all Legitimate Interests Assessments (LIAs).
<b>Criminal Offence Data</b> – to process personal data about criminal convictions or offences, you need to show one of the five bases above and either legal authority or official authority for the processing of such data.
<b>Retention period</b>
Seven Years to comply with contracted FCA Regulations
<b>Source of the data (if not collected from the data subject)</b>
<ul style="list-style-type: none"> <li>• Client Representative (Manager/HR/Colleague/Insurance Broker/Next of Kin/GP)</li> <li>• Client Contract</li> <li>• Insurance Policy</li> <li>• Medical Facility</li> </ul>

<b>In which locations does the processing take place</b>
<ul style="list-style-type: none"> <li>• NGS Ops London</li> <li>• Client Head Office/Regional Office</li> <li>• Service Provider EU</li> <li>• Service Provider outside the EU</li> <li>• Compliant backup data centres in the EU and NA1</li> </ul>
<b>Any regulated automated decisions taken</b>
No
<b>How we process your data and where it is held.</b>
<ul style="list-style-type: none"> <li>• Data Collection <ul style="list-style-type: none"> <li>• Initial tasking detail</li> <li>• Situation interrogation</li> <li>• Additional information gathers</li> <li>• Consent for medical in confidence</li> <li>• Hardcopy communications portals (post/fax) will be sanitised as soon as required data is transferred to Salesforce casefile.</li> </ul> </li> <li>• Storage <ul style="list-style-type: none"> <li>• Calls – VOIP Server – Salesforce casefile and/or account record – Secondary back up servers</li> <li>• Emails – Mail Server – Salesforce casefile, account and contact record - Secondary back up servers</li> <li>• Documents and Reports - Mail Server, Salesforce casefile, account and contact record - Secondary back up servers</li> <li>• Case financials - Mail Server, Xero, Salesforce casefile, account and contact record, Word pay - Secondary back up servers – Hard copy records</li> </ul> </li> <li>• Usage <ul style="list-style-type: none"> <li>• Client verification</li> <li>• Situation validation</li> <li>• Resolution options to pre-identified service providers</li> <li>• Client management</li> <li>• Internal/External audit</li> <li>• Accountancy functions, billing and paying</li> </ul> </li> <li>• Deletion <ul style="list-style-type: none"> <li>• Full erasure on verified request</li> <li>• Full erasure in accordance with contractual obligations</li> <li>• Full erasure in accordance with legal obligations</li> </ul> </li> </ul>
<b>What are the risks:</b>
<ul style="list-style-type: none"> <li>• Inadequate controls increase the likelihood of information being shared inappropriately</li> <li>• Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk</li> <li>• Accuracy of data subject information can pose a physical risk if out of date, incorrect or incomplete</li> <li>• Third Countries outside of the EU may not be compliant with GDPR and sharing information to providers outside the EU may not provide appropriate safeguards for the protection of personal information</li> </ul>

**Data Subject Access Procedure**

Data Subject Access Request forms (DSAR) can be downloaded from our website:

[www.northcottglobalsolutions.com](http://www.northcottglobalsolutions.com) - **\*Verbal requests are not valid.**

Completed forms should be emailed to: [dataprotection@northcottglobalsolutions.com](mailto:dataprotection@northcottglobalsolutions.com)

Posted to: Data Protection Officer, Northcott Global Solutions, 22 Bevis Marks, London, EC3A 7JB

Faxed to: +44 (0)207 183 8919

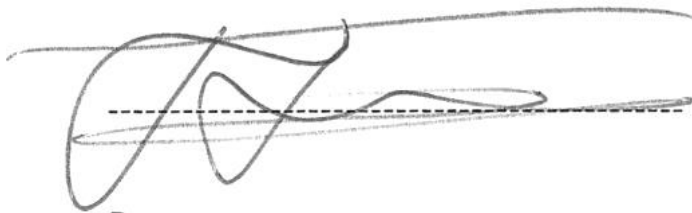
On receipt of completed DSAR form, NGS's Data Protection Officer will verify the request in line with DPA 2018 regulations and action in adherence to regulations and internal policies.

**As a Data subject, you have the following rights:**

- Right of rectification – you have a right to correct data that we hold about you that is inaccurate or incomplete.
- Right to be forgotten – in certain circumstances you can ask for the data we hold about you to be erased from our records.
- Right to restriction of processing – where certain conditions apply, to have a right to restrict the processing.
- Right to object to processing – you have the right to object to certain types of processing such as direct marketing.
- Right to lodge a complaint – if you are not satisfied with how your personal data is being processed by Digital Asset Management (or third parties), or how your complaint has been handled, you may lodge a complaint directly with the supervisory authority and Digital Asset Management's CEO.
- No automated profiling will be used in the processing of your personal data. It will only be used for the purpose it was gained and human intervention is the only way NGS will process your personal information

**Date:** 10<sup>th</sup> March 2020

EDWARD NORTHCOTT JONES

A handwritten signature in black ink, appearing to read 'Edward Northcott Jones', written over a horizontal dashed line.

**Signature:**

CEO