GDPR - Data Processing Customer Statement

This document is provided by Next Connex (which may be defined under the terms of the General Data Protection Regulation (to become Data Protection Bill when passed) as a Data Processor for some of the services we provide), to our Data Controller customers to comply with our duty to assist with definitions and duties as defined in Recital 95 of the General Data Protection Regulation, with comprehensive coverage within Chapter IV.

Its purpose is to define the level of compliance within our organisation and to address any areas that require attention prior to 25th May 2018. It may assist you to review as a starting record the compliance that data processors will be required to cover under article 28.

It is our belief that, as a network and co-location infrastructure provider, we are not a Data Processor. However, our Data Controller customers may wish to have clarification of the relationship which is defined in the statement below. We have a duty to ensure that our security arrangements are at least equivalent to the security that you are required to have in place as if you were processing the data yourselves. Please refer to the full requirements that we will be satisfying within Article 28 of GDPR.

We would advise that for these purposes our Data Protection Officer support is provided through Satswana Ltd. who can be contacted at info@satswana.com - Reference Next Connex DPO.

1. We would advise that your data may pass across our network and where applicable is stored within systems provided by us under the terms of our commercial contract with you, available as a separate document.
2. None of our staff has permission to access the data, either internally or externally.
3. Access to our core network infrastructure that your data may pass across is logged and controlled.
4. Where applicable your data is backed up as per the requirements in your commercial contract referenced in Point 1.
5. You may have opted to have your data encrypted on our servers.
6. It is only decrypted when accessed according to your policies.
7. We do not apply anonymisation or pseudonymisation - that is under your control if required.
8. The data retention policy is set by you.
9. We do not process your information in any form.
10. We are not involved in any manner in which you update personal information.
11. We have no means of knowing whether any of the information that is processed is incomplete, outdated or wrong. That is a matter for your control.
12. We offer no mechanism for a data subject to access the data, and thus they cannot correct it. This control is solely through your access.
13. We do not sell or rent any personal information to third parties. We may disseminate your personal information where required for the delivery of your services – as per your commercial contract referenced in Point 1.

14. We have no mechanism to check the accuracy and completeness of data, which is solely under your control.
15. All processes to update, correct or delete data are under your control.
16. We do not operate any regular or automated process to 'clean' data.
17. If any dataset included personal information on subjects under the age of 16 then we would have no means of knowing that, all data classification is under your control.
18. Personal data would never get transferred to another party by us except as part of the commercial contract referenced in Point 1.
19. We would not be aware if any dataset included recordings of video or sound that included the public.
20. We confirm that information (digital, manual and especially special category data) as provided by you is only stored in our organisation. Any third party (Sub-Processor) involvement is provided for within our commercial contract referenced in Point 1.
21. Any separate handling and storage of special category data is subject to your decision and your policy.
22. Archived information is stored as agreed within the terms of our commercial contract referenced in Point 1.
23. All physical, administrative and technological security procedures in operation to keep your information secure are managed under our ISO/IEC27001:2013 Information Security Management System.
24. Nobody within or outside our organisation has access to your personal information except as part of the commercial contract referenced in Point 1.
25. We have policies and procedures for dealing with breaches which can be identified and reported to the Data Controller within 72 hours.
26. The data audit facilities and controls that are in place to ensure that there is no internal unauthorised access to personal data is subject to our ISO/IEC27001:2013 Information Security Management System.
27. We have a process for the destruction of personal information, including backups and archives when instructed to do so by the Data Controller except where this data passes across our network which is a matter for your control.
28. You authorise the destruction, which is executed as in 27 above.
29. At the end of the contract period all data is destroyed as in 27 above.
30. We are not required to transfer data between departments or to third parties except as part of the commercial contract referenced in Point 1.
31. We confirm that no data including archives and backups is transferred outside the UK and EEA. Any of your data that passes across our network to destinations outside the UK and EEA does so under your sole control.
32. We have a privacy policy as published on our website- www.nextconnex.com
33. We confirm that we are prepared to enter into a contract with you as required by GDPR as below:

a. Processing by a processor must be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, categories of individuals whose data is being processed and the obligations and rights of the controller. The contract must stipulate, in particular, that the processor will:
b. Process only on documented instructions, including regarding international transfers (unless, subject to certain restrictions, legally required to transfer to a third country or international organisation);
c. Ensure those processing personal data are under a confidentiality obligation (contractual or statutory);
d. Take all measures required under the security provisions (Article 32) which may include pseudonymising and encrypting personal data as appropriate;
e. Only use a sub-processor with the controller's consent (specific or general, although where general consent is obtained processors must notify changes to controllers, giving them an opportunity to object); flow down the same contractual obligations to sub-processors;
f. Assist the controller in responding to requests from individuals (data subjects) exercising their rights;
g. Assist the controller in complying with the obligations relating to security, breach notification, DPIAs and consulting with supervisory authorities (Articles 32-36);
h. Delete or return (at the controller's choice) all personal data at the end of the agreement (unless storage is required by EU/member state law);
i. Make available to the controller all information necessary to demonstrate compliance; allow/contribute to audits; and inform the controller if its instructions infringe data protection law.

We look forward to being of further service to you.