Data Protection Agreement

This Data Protection Agreement (hereinafter referred to as the "Data Protection Agreement") is entered into on April 26, 2013 ("Effective Date") by and between Business Objects Software Limited, a company incorporated in Ireland having its registered office at 1012 - 1014 Kingswood Avenue, City West Business Campus, Dublin 24, Ireland ("BOSL") and SAP Labs Israel Ltd.,., a company incorporated in Israel, having its registered office at 15 Hatidhar St., 43665 Ra'anana, Israel (hereinafter "Contractor").

WHEREAS Contractor provides maintenance and support services to BOSL, its worldwide subsidiaries and channel partners; and further, on behalf of any of the aforementioned entities, to end users of BOSL products and services; AND

WHEREAS the provisioning of such maintenance and support services implies the possibility of a transfer to and the processing by Contractor of personal data controlled by the respective end users ; and/or the possibility that Contractor may have access to such personal data while providing services on the systems of the respective end users; AND

WHEREAS the parties acknowledge and agree that the services of Contractor under the Agreement in such circumstances would constitute contractual data processing by Contractor under EU Directive 95/46/EC (hereinafter referred to as the "Data Protection Directive") and data protection laws of EU and EEA Member States applicable to the respective end users of the serviced BOSL products and services; AND

WHEREAS the Data Protection Directive and applicable data protection law of EU and EEA Member States stipulate that carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating that the processor shall (i) act only on instructions from the controller and (ii) have implemented certain technical and organizational security measures; AND

WHEREAS pursuant to the Data Protection Directive a transfer of personal data to a non-EU/EEA country for processing may only take place if an adequate level of protection is ensured; AND

WHEREAS the European Commission has adopted, by Commission Decision of 5 February 2010 (2010/87/EU), a set of standard contractual clauses for the transfer of personal data to processors established in non-EU/EEA countries (hereinafter referred to as the "Clauses"); AND

WHEREAS these Clauses are considered by the European Commission as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals;

NOW THEREFORE, in order to comply with the requirements of the Data Protection Directive and applicable data protection laws of the EU and EEA Member States,

THE PARTIES HAVE AGREED to the Clauses attached hereto as Annex 1, subject to the following Additional Terms:

1 Personal Data controlled by BOSL

1.1 To the extent that Contractor provides maintenance and support for BOSL's own systems and personal data controlled by BOSL are transferred to Contractor for processing, the Clauses as detailed in Annex 1 shall apply directly and BOSL shall be the 'data exporter' and Contractor the 'data importer' of such personal data. The same shall apply accordingly where for the purposes of providing maintenance and support to BOSL Contractor accesses data processing systems. operated by or on behalf of BOSL and these systems may contain personal data controlled by BOSL.

1.2 Governing law, per Clause 9 of the Clauses, in cases described in Section 1.1~~1.1~~ shall be German law.

2 Personal Data controlled by other end-users

2.1 BOSL's worldwide subsidiaries, channel partners and any end-users to whom Contractor provides maintenance and support services (hereinafter collectively referred to as "Other Controllers") may accede to this Data Protection Agreement as controllers with respect to any personal data controlled by them and Contractor. In such case the Clauses in Annex 1 shall apply as if they had been entered into directly by and between the respective Other Controller being the 'data exporter' and the Contractor being the 'data importer'.

2.2 Other Controllers may declare their accession to this Data Protection Agreement by submitting a written declaration of accession to BOSL. The declaration of accession shall specify the governing law per Clause 9 of the Clauses and further include contact information of the acceding Controller's data protection officer and/or other persons to contact with respect to any notification obligations under the Clauses.

2.3 BOSL will promptly notify Contractor of any accession by a new Controller to this Data Protection Agreement.

2.4 Each Controller may terminate its participation in this Data Protection Agreement for convenience by written declaration towards BOSL, with three months prior written notice. The Controllers' right to terminate for cause shall remain unaffected, as shall the right to immediately cease providing personal data for processing under this Data Protection Agreement. BOSL will promptly notify the Controller of the termination. The validity of the Data Protection Agreement shall not be affected by the termination of individual Controllers; it shall be continued among the other Parties.

3 Compliance Audits by BOSL

3.1 Contractor agrees that BOSL, in addition to BOSL's and/or any other individual Controller's audit rights under the Clauses, may audit Contractor's overall compliance with the terms of this Data Protection Agreement and the technical and organizational security measures implemented by Contractor (as documented in Appendix 2 to the Clauses) at any time. Such audit may be carried out by BOSL or its internal or external auditors and shall be carried out during normal business hours without disruption to the business of Contractor.

3.2 Contractor will conduct regular internal audits with respect to the technical and organizational security measures specified in Appendix 2 to the Clauses and will submit the audit reports to BOSL without delay.

3.3 Contractor agrees that BOSL may disclose the findings of and audits made pursuant to Sections 3.1~~3.1~~ and 3.2~~3.2~~ to the other Controllers.

4 Miscellaneous

4.1 If any provision in this Data Protection Agreement is ineffective or void, this shall not affect the remaining provisions. The parties hereto shall replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. The parties shall similarly add a necessary appropriate provision where such a provision is missing.

4.2 This Data Protection Agreement, excluding the attached Clauses, may be modified only by a written amendment signed by both parties. This Data Protection Agreement prevails over any additional, conflicting, or inconsistent terms and conditions appearing on any document submitted by either party regarding the subject of this Data Protection Agreement.

4.3 In each instance in which provisions of the Additional Terms contradict or are inconsistent with the Clauses, the Clauses shall prevail and govern and the contradicted or inconsistent provisions of the Additional Terms shall be deemed amended accordingly.

4.4 This Data Protection Agreement shall apply regardless of whether Contractor is established within or outside the European Union or a country recognized, within the meaning of the Data Protection Directive, by the Commission as providing adequate protection or a third country.

4.5 BOSL and Contractor each may terminate this Data Protection Agreement for convenience by written declaration to the other Party, with three months prior written notice to the end of the calendar year. The Parties' right to terminate for cause shall remain unaffected, as shall BOSL's right to immediately cease providing personal data for processing under this Data Protection Agreement. BOSL will duly notify the other Controllers of a termination by Contractor.

SIGNATURE PAGE FOLLOWS

Both Parties accept the terms of this Data Protection Agreement by signing below.

AGREED TO

BOSL	Contractor
Name (written out in full): Dympna Donnelly	Name (written out in full): Mickey Stemler
Position: Director	Position: Managing Director
Date: 15 May 2013.	Date: May 2, 2013
Signature: Dympna Donnelly.	Signature: M. S.
Name (written out in full):	Name (written out in full):
Position:	Position:
Date:	Date:
Signature:	Signature:

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)[1]

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

BOSL or the respective other Controller,
as defined by Sections 1 and 2 of the Additional Terms

(in the Clauses hereinafter referred to as the '**data exporter**')

and

Contractor

(in the Clauses hereinafter referred to as the '**data importer**')

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of

[1] Pursuant to Commission Decision of 5 February 2010 (2010/87/EU)

personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7,Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data

exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually

disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely Germany.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer

warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter enjoys maintenance and support services provided by the data importer for BOSL products and services. The provisioning of such maintenance and support services implies the possibility of a transfer to and the processing by the data importer of personal data controlled by the data exporter; and/or the possibility that the data importer may have access to such personal data while providing services on the systems of the respective data exporter.

Data importer

The data importer provides maintenance and support services to the data exporter.

Data subjects

The personal data transferred concern the following categories of data subjects:

☑ Employees of
- ☑ BOSL
- ☑ customer
- ☑ vendor/supplier
- ☑ partner

☑ Customer of
- ☑ BOSL
- ☑ customer

Categories of data

The personal data transferred concern the following categories of data (mark all applicable)

☑ Personal Details
☑ HR Data
☑ Salary and Social Security Data
☑ Contract and Invoice Data
☑ Bank Account data, Credit or Debit Card Data
☑ Qualification /Education Details
☑ System Access / Usage / Authorization Data

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (mark all applicable)

☑ Race and Ethnic Origin
☐ Political Opinions
☑ Religious or philosophical beliefs, trade union membership
☑ Physical or mental health
☐ Sexual life

☐ Accusations incl. suspicions ☐ Criminal offences, convictions and judgements

☐ Internet usage and web tracking information (e.g. cookies)

☐ Rating and Quality Score Data

Processing operations

The personal data transferred will be subject to the following basic processing activities:

Provision of incident, problem management and remote support services by data importer.

BOSL	**Contractor**
Name (written out in full): DIARMUID DOHERTY	Name (written out in full): Mickey Stelma
Position: DIRECTOR	Position: Managing Director
Date: 15 MAY 2013.	Date: May 2, 2013
Signature:	Signature:
Name (written out in full):	Name (written out in full):
Position:	Position:
Date:	Date:
Signature:	Signature:

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

General Description of Measures Taken by BOSL:

At BOSL, personal data is handled and protected in a way that is designed to:

- Maintain confidentiality (only authorized persons receive access);
- Safeguard integrity (only authorized persons can change the personal data); and
- Maintain availability (where personal data is stored within BOSL as part of its contractual obligations, the information is available within the bounds defined by the owner of information).

As part of the BOSL Policies, the BOSL executive board has established a global BOSL Security Policy, which is a binding guideline for wholly-owned subsidiaries within the BOSL Group and their employees. The BOSL Security Policy governs the fundamental aspects of the security measurements at BOSL for protecting its employees, assets, information and systems. It also forms the basis for the security measures to be taken in the specific business areas and BOSL companies. Through the BOSL Security Policy, every employee and third-party contractor accessing BOSL's system is made aware of his/her responsibility with regard to BOSL's security guidelines and is obligated to be proactive in exercising such responsibility. The BOSL Security Policy also defines BOSL's security objectives and outlines those set out in specific security standards. Such security standards provide instructions for specific areas of security (e.g. data protection, facility access restriction, virus protection) that enable BOSL employees to implement the security requirements.

All BOSL employees and third-party providers of BOSL are obliged to comply with the BOSL Security Policy and observe the security standards contained therein.

All BOSL employees and all third party personnel providing services to BOSL and having access to data is obliged in writing to observe data secrecy according to applicable law.

In the following sections, the minimum measures are defined. BOSL is free to enhance and improve measures at any time in accordance with the terms and conditions of the Agreement. This may also lead to a replacement of specific measures by other equally effective measures to achieve the same goals.

Measures Specific to support services provided by BOSL's support centers:

Access Control: Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms where data processing systems are located which process personal data.

Measures:

BOSL protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.

In general, buildings are secured through access control systems (smart card access system).

As a minimum requirement, the outermost shell of the building must be fitted with a certified master key system including modern, active key management.

Depending on the security classification, buildings, individual areas and surrounding premises will be further protected by additional measures: These include specific access profiles, closed circuit TV, intruder alarm systems, and even biometric access control systems. A separate access control concept, which includes documentation of names, is used data centers.

Access rights will be granted to authorized persons on an individual basis according to the defined criteria. This also applies to visitor access. Guests and visitors to BOSL buildings must register their names at reception, and must be accompanied by company personnel.

BOSL employees and external personnel must wear their ID cards at all BOSL locations.

System Access Control: Data processing systems must be prevented from being used without authorization.

Measures:

Multiple authorization levels are used to grant access to sensitive systems. Processes are in place to ensure that authorized users have the appropriate authorization to add, delete, or modify users. All users access BOSL's system with a unique identifier (user ID).

BOSL has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user leaves the company, these access rights are rescinded.

BOSL has a password policy that prohibits the sharing of passwords, governs what to do if a password is disclosed, and requires passwords to be changed on a regular basis. Personalized user IDs are assigned for authentication. All passwords are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months. This complies with the requirements for complex passwords. BOSL ensures that default passwords are changed on networking devices. Each computer has a password protected screensaver.

The company network is protected from the public network by a hardware firewall.

BOSL uses antivirus software at access points to the company network (for e-mail accounts) and on all file servers and all workstations.

Security-relevant updates for the existing software are regularly and automatically downloaded and installed.

Remote support: Access to data exporter systems per default occurs via remote access. Therefore access to data exporter's systems is controlled by security measures implemented in data exporter's systems and subject to data exporter's compliance and audit processes. Accessing data exporter's systems is only possible after an authorized employee of data exporter has granted the necessary permissions.

Data Access Control: Persons entitled to use data processing systems shall gain access only to the data which they have a right of access and personal data must not be read, copied, modified or removed without authorization in the course of processing.

Measures:

Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information they require in order to complete their work. BOSL uses authorization concepts that document how authorizations are assigned and which authorizations are assigned. All personal, confidential, or otherwise sensitive data is protected in accordance with the relevant security standards. Confidential information must be processed confidentially.

All production servers are operated in the relevant data centers/server rooms. The security systems that protect applications for processing personal, confidential or other sensitive data are regularly checked. To this end, BOSL conducts internal and external security checks and penetration tests on the IT systems.

BOSL does not allow the installation of personal software or other software not approved by BOSL. An BOSL security standard governs how data and data carriers that are no longer required are deleted or destroyed.

Data Transmission Control:

Except as necessary for the provision of the services in accordance with the service agreement, personal data must not be read, copied, modified or removed without authorization during transfer or storage and it shall be possible to establish to whom personal data was transferred to.

Measures:

Data that is transferred from the BOSL network to other external networks is encrypted. Where data carriers are physically transported, adequate measures must be taken to ensure the agreed service levels (for example, encryption, lead-lined containers, and so on).

Data Input Control: It shall be possible retrospectively to examine and establish whether and by whom personal data have been entered into data processing systems, modified or removed.

Measures:

BOSL only allows authorized persons to access personal data as required in the course of their work. As part of the support delivery process, the access to customer systems by users and administrators is recorded in a log file.

Job Control: Personal data being processed on commission shall be processed solely in accordance with the service agreement and related instructions of the client.

Measures:

BOSL uses controls and processes to ensure compliance with contracts between BOSL and its service providers.

As part of the BOSL security policy, no customer information is classified lower than "confidential".

Access to customer data systems is usually granted via remote support. This is governed by the following security requirements:

In general, the remote internet connection is established via a Secure Network Communications (SNC) or Virtual Private Networks (VPN) connection. Both options use various security measures to protect customer systems and data from unauthorized access: These include strong encryption, user authentication, and access control technology.

The Secure Area is a specially designated support ticket facility in which BOSL provides a special access-protected and monitored security area for transferring the access data and password.
At all times, BOSL customers have control over their remote support connections. BOSL employees cannot access a customer system without the knowledge or full active support of the customer.
All BOSL employees and contractual partners are contractual bound to respect the confidentiality of all sensitive information including information about the trade secrets of BOSL customers and partners.
During the support process, the personal data of different customers is physically or logically separated.

Availability Control: Personal data shall be protected against disclosure, accidental or unauthorized destruction or loss.

Measures:

BOSL employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary. BOSL also uses uninterrupted power supplies (UPS, batteries, generators, and so on) to ensure power is available to the data centers. Emergency processes and systems are regularly tested.

Firewalls or other network security technologies are also used. In accordance with the security policy, regularly updated antivirus products are also available on all systems.

Multi Entity Separation Control: Access to data exporter systems per default occurs via remote access and there is no processing of personal information on BOSL owned systems. Separation of multiple entities/clients in context of data processing and storage in such cases is enforced by data exporter. Where data or an entire system is transferred over to BOSL, BOSL uses the technical capabilities of the deployed software (multi tenancy, separate system landscapes) to bring about data separation. If personal data is required to process a message, the data is assigned to that message and used to process that message only; it is not accessed to process any other message. Such data is stored in dedicated support systems.

SIGNATURE PAGE FOLLOWS.

BOSL	Contractor
Name (written out in full): DYMPNA DONNELLY	Name (written out in full): Mickey Stelmer
Position: DIRECTOR	Position: Managing Director
Date: 15 MAY 2013.	Date: May 2, 2013
Signature: Dympna Donnelly	Signature: M. [illegible]
Name (written out in full):	Name (written out in full):
Position:	Position:
Date:	Date:
Signature:	Signature: