Supplier
Security Standard
v4

Introduction

Sky, in common with all Data Controllers, is required under relevant data protection legislation to ensure that "appropriate technical and organisational measures" are taken to protect personal data that it has been entrusted with. To achieve this, Sky has established this Security Standard.

This standard sets out the objectives behind the security that Sky expects of its suppliers and business partners when they are entrusted with handling Sky Data. Sky requires these specific minimum standards to be implemented across a supplier's environment and infrastructure.

This document forms part of the Agreement entered into between a Supplier and Sky and as such sets out the security obligations that Sky places on Suppliers in relation to the protection of Sky personal data.

All Suppliers who process Sky personal data are categorised by Sky as either "Tier 1" or "Tier 2", depending on the type of personal data that is being processed. "Tier 3" Suppliers are those Suppliers who do not process any personally identifiable data. Guidance on the application of these definitions can be found in Appendix 4. The "Tier" classification of a Supplier will determine the level of due diligence that a Supplier will need to apply..

We draw attention to the fact that a Supplier, who is originally classified as Tier 2 but then, by virtue of receiving additional data in the course of providing the Services or there are changes to the Services provided, becomes the holder of Tier 1 data will be expected to adhere the Tier 1 due diligence requirements before receiving the new data or providing the additional Services.

We also draw attention to the fact that the requirements of the Security Standard apply only to those locations and associated systems and controls that are used to process Sky personal data. This means that, if a Supplier has multiple locations, only those that are used to process Sky personal data are in scope, and for systems, only those systems used to process Sky personal data are required to be covered.

Due Diligence Requirements for Suppliers with access to Sky personal data

Tier 1 Suppliers

Suppliers who are categorised by Sky as "Tier 1" Suppliers are those with access to Sky's Secret Data (information, which if lost or wrongly disclosed could cause very serious damage to the interests of Sky, its customers, people, suppliers and business partners).

Tier 1 Suppliers must, at their own cost, obtain annual independent certification to demonstrate that the operation of their controls meet the obligations set out in this Security Standard.

The independent certification must be provided by the Supplier to Sky prior to the initial receipt of any Sky personal data, and then annually in accordance with the timetable communicated to the supplier by Sky's Audit, Risk Management and Compliance department ("ARMC").

The review to support such independent certification should be conducted against appropriate professional standards and be delivered against the International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organisation", an SSAE16 report or a report in an equivalent format.

The audit reports for new Suppliers should be "type 1", as at a point in time, to demonstrate that controls are in place prior to the supplier receiving Sky personal data and, in subsequent years, a "type 2" form is required which confirms the operation of the controls over the preceding 12 month period.

The reports must set out the controls that are in operation to demonstrate compliance with the standards set out in this document and specify the testing that has been performed by the independent verifier and the results.

The review should be commissioned directly by the Supplier, at its own cost, and should, after the initial submission, be carried out every 12 months or to a timetable agreed in advance with ARMC. The report should be executed by PwC, EY, Deloitte, KPMG or Grant Thornton.

A Supplier who intends to use an alternative verifier must contact Sky in advance to confirm that the verifier is acceptable to Sky.

The terms used in this standards document are defined in Appendix 1.

Tier 2 Suppliers

Suppliers who are categorised by Sky as "Tier 2" are those with access to Sky's Confidential Data (personal information that can be traced to individual customers; information which if lost or wrongly disclosed could cause distress to Sky's customers or people, or damage the interests of Sky).

The Supplier's compliance with these Tier 2 requirements, as they apply to personal data, will be assessed by ARMC. This work will be performed prior to a Supplier being given access to Sky personal data and will entail, at a minimum, an assessment of the supplier's responses to this Security Standard and may include an on-site audit by members of ARMC, depending on the type of data to be held, and the volume.

The process to be followed will already have been set out in writing by your Sky Business Relationship Owner.

ARMC is happy to work with suppliers to address any issues or questions that arise as a result of or in the completion of this checklist or where potential or actual non-compliance with this Security Standard is identified.

Where the Supplier holds external validation or certification over the systems and processes that will be used to protect Sky's personal data such as an SSAE16 or equivalent, a copy should be provided to Sky in addition to the supplier's responses to this Security Standard.

Suppliers will be required to complete an annual recertification when requested by ARMC, which may also involve an on-site visit by members of ARMC, in accordance with Sky's policy of visiting all suppliers who hold Sky personal data as part of a rolling programme of audits.

Suppliers in Germany and Italy

Specific provisions, applicable to only Suppliers providing services to Sky Deutschland, Austria and /or Sky Italia, are set out in Appendix 5 and Appendix 6 and these should be read in conjunction with the main standards where applicable.

Sky Security Standards for Suppliers

1. Policies and Codes of Conduct

1.1. The Supplier shall provide a copy of their employee codes of conduct or similar document(s) covering anti-bribery and corruption, whistle-blowing and other appropriate ethics policies (such as anti-money laundering and anti-slavery) that are in place and be able to demonstrate that these have been clearly communicated to all relevant staff.

1.2. The Supplier shall be required to show that there are mechanisms in place to ensure ongoing compliance with these policies and to identify and action any acts or areas of non-compliance.

2. Data Protection Governance

2.1. Accountability for data protection across all jurisdictions is clearly assigned to a designated individual or other body with appropriate seniority within the Supplier's company.

2.2. A clear data protection policy, which includes retention and destruction times, is in place and communicated to all relevant staff.

2.3. The Supplier will agree its proposed retention period for Sky personal data with Sky in writing.

2.4. Processes are in place to ensure and demonstrate compliance with the data protection policy.

2.5. A training log is maintained by the Supplier illustrating that all relevant staff with access to Sky personal data have successfully completed data protection training.

2.6. The Supplier has a process to authorise the receipt of reports that the Supplier intends generating that contain Sky personal data.

2.7. Processes are in place to advise Sky of any data protection or security breaches(i) in a timely fashion and (ii) in accordance with local legislative requirements where there is an obligation to notify a regulator.

2.8. Confirmation should be provided by the Supplier to Sky that there have been no unreported data breaches in the preceding 12 month period.

3. Notice, Choice and Consent

3.1. The Supplier will notify Sky in writing if the type of data changes from what was originally intended to be processed under an agreement , prior to any change occurring.

3.2. The Supplier will agree with Sky in advance and in writing if the supplier is to perform additional processing of Sky personal data.

3.3. The Supplier will provide individuals, whose personal data is likely to be further processed, with an additional privacy notice before such additional processing. This additional privacy notice will specify how the Supplier intends further to process the data and for what specified purpose.

3.4. The processing of Sky personal data will be justified either:

- through having obtained the consent of the individuals; or
- by another legitimate interest, notified to and agreed by Sky in advance of the change, who will then issue revised written instructions to the Supplier regarding the processing of that Sky personal data.

4. Data Collection

4.1. Data collected and/or processed by the Supplier is restricted only to that which is required to fulfil the Supplier's provision of the Services to Sky and there are appropriate controls in place to ensure and demonstrate that this is the case

4.2. Where marketing activities are carried out by the Supplier on Sky's behalf, such marketing must be carried out in accordance with Sky's privacy notice and within the scope of the individuals' permissions. If the Supplier is managing the consent process, it will be required to evidence such scope and permissions for each individual.

4.3. There are controls in place to ensure that Customer's chosen marketing preferences are adhered to.

4.4. Where web sites are used to collect Sky personal data and/or cookie codes, this is done in accordance with the privacy notice displayed on the website and any other applicable privacy and cookie statements in accordance with relevant legislation.

4.5. There is a policy explaining how the Supplier uses personal data and cookies (if they are used) which is displayed to customers.

4.6. The Supplier will notify Sky if it intends to process Sky personal data in such a way as to aggregate and/or anonymise the data for the Supplier's own use.

4.7. The Supplier will obtain permission from Sky, in writing, if it intends to process or otherwise make use of Sky personal data for any purpose other than that which is directly required for the supply of the Services.

5. Subject Data Access

5.1. Data subjects have the right to a copy of the data an organisation holds about them. Supplier Personnel are aware of how to identify a subject access request ("SAR") and what to do when they receive a SAR. This includes notifying Sky, where relevant, within an appropriate period and in compliance with any regulatory requirements in place and agreeing a mechanism to respond to the SAR.

5.2. The Supplier has the requisite functionality on all systems which will hold Sky personal data to enable the Supplier to comply with SARs within the appropriate time period.

6. Data disclosure to Third Parties (including Subcontractor Management)

6.1. Where Sky personal data will be processed by the Supplier's third parties, including Subcontractors/Sub-processors, the Supplier will provide Sky with:

- A list of all third parties;
- What data will be accessible by them; and
- How the supplier will ensure the data is kept secure.

This includes, for example, outsourced data centres or cloud providers. Pre-approval by Sky, in writing, of any change in third parties is required.

6.2. Where Sky personal data is processed by a third party on behalf of the supplier, written contracts or letters of appointment as data processors or sub-processors are in place with all such third parties to cover disclosure and data security requirements.

6.3. The Supplier will be able to demonstrate whether those third party contracts require the third parties to have in place an equivalent level of data security as set out in this Security Standard and how the supplier ensures this is the case.

6.4. Where the third party is found, by the Supplier , to be deficient in any area of data security, the supplier must notify Sky and provide additional information for example, details as to the deficiency, mitigating reasons therefor and plans to rectify

6.5. If Sky personal data will be accessed from outside the European Economic Area, there is a written agreement in place covering such processing. This agreement would include, for example, details as to where data or backups are processed by staff in outsourced data centres and the standard contractual clauses or binding corporate rules (as approved by the European Commission).

6.6. The Supplier has a contractual obligation to obtain assurance over the data security of all Subcontractors and sub-processors who will hold Sky personal data.

6.7. The Supplier has, in terms of its obligations to ensure that its sub-processors are taking appropriate technical and organisational measures, conducted a review of the Subcontractor in the past; or

6.8. The Supplier intends to conduct a review if the Subcontractor is new under the proposed agreement and the Supplier will notify Sky by when such review will be conducted.

6.9. The Supplier maintains a register of data protection breaches that have arisen at Subcontractors.

6.10. All complaints relating to personal data are captured and recorded by the Subcontractor and notified to the Supplier on a timely basis. The Supplier will notify any relevant complaints to Sky within an agreed period and in compliance with any regulatory requirements in place.

7. Personnel Security

7.1. Where appropriate to the nature and classification of data handled by the supplier, or as agreed with Sky, screening checks may be conducted on Supplier Personnel including reference checks and, where applicable, financial probity checks (please see Appendix 3). As appropriate to the job role and as permitted by law, criminal record checks are to be conducted (please see Appendix 2).

7.2. Where appropriate, these checks are refreshed on a periodic basis.

7.3. The results are logged and recorded.

7.4. All Supplier Personnel sign an agreement which requires them to keep information confidential. This also covers all Sky personal data

7.5. The supplier has a comprehensive code of conduct in place which includes requirements for personnel to demonstrate awareness of procedures around breaches of security, including breaches of data security.

7.6. Supplier Personnel are required to agree to adhere to all Supplier company policies, rules and procedures, including applicable data protection policies.

7.7. There is a clear process to handle Supplier Personnel who terminate their services with the Supplier.

7.8. The Supplier has a policy to remove access to Sky Personal data from those Supplier Personnel within an appropriate timeframe.

7.9. The Supplier has a policy to remove access to access to Sky personal data from Supplier Personnel who have changed roles and no longer require access.

8. Physical and Environmental Security

8.1. Responsibilities for physical security and risk management are clearly defined by the Supplier and are allocated to an individual or body within the supplier with sufficient authority.

8.2. The Supplier has a clearly defined physical security policy and related standards.

8.3. The requirements of the physical security policy are applied to all locations that will be used to support Sky operations.

8.4. Access to all entry points at all locations where Sky personal data will be processed is restricted and logged so that it can be reviewed.

8.5. Unless otherwise agreed with Sky, telecommunications areas and data centres, reception areas, exit/entry points, and vulnerable or confidential working are covered by an internal and external CCTV system which is used and monitored.

8.6. The Supplier shall provide and maintain secure physical premises that provide a safe working environment which adequately protect against loss or damage to the premises or to the equipment.

8.7. The Supplier shall implement uninterruptible power supplies ("UPS") for critical infrastructure and shall test the UPS regularly.

8.8. The Supplier shall ensure that all power supplies and fire safety mechanisms undergo regular maintenance checks and that facilities comply with appropriate health and safety standards.

8.9. Where Sky personal data is stored or processed, the supplier shall provide sufficient secure storage space for personnel to store those personal effects that are capable of copying data.

8.10. The Supplier shall ensure that prominent security signage or information in suitable electronic form detailing security policies and requirements are provided or displayed in all relevant locations.

8.11. The Supplier will not perform the Services to Sky from other Sites, without obtaining the prior written consent of Sky as far as reasonably practicable, without causing any material disruption to the business of Sky or the provision of the Services.

8.12. Where a shared Site is in operation, the Supplier shall:

- as a minimum, segregate or 'ring-fence' the area in which the Services take place for Sky or advise Sky in advance if this is not possible; and
- ensure that the Services and facilities required to provide the Services to Sky allow Sky's data to be separately identified from the Supplier's other customers.

8.13. A clear desk policy is operated at all Sites.

9. Incident Response

9.1. All security incidents are logged with their origin and resolution recorded.

9.2. There is a clear escalation process within the Supplier and a notification to Sky where necessary.

10. Business Continuity and Disaster Recovery

10.1. There are business continuity and disaster recovery plans in place. Disaster recovery plans must ensure the restore of the access to data in accordance with contractually agreed Return To Operation and in any case within 7 days.

10.2. The plans are tested annually or at such other frequency required by Sky and agreed by the parties.

10.3. Backups are taken and recovery is tested on a regular basis, are encrypted and securely transported if taken off-site.

10.4. Capacity monitoring is in place for those systems that support the Supplier's provision of the Services to Sky.

11. Information Security

11.1. Supplier systems that will be used to transmit, collect, receive, process and/or store Sky personal data adhere to the Supplier's information security policy and the Supplier will provide a copy to Sky.

11.2. The Supplier's information security policy and the associated controls in operation include but are not limited to:

- Network and perimeter security
- Protection of malicious code
- Encryption (where applicable to services)
- Masking of personal data (for financial transactions)
- Patching

11.3. All Sky personal data is transferred or exchanged via secure channels which are appropriately encrypted according to industry standards.

11.4. All Sky personal data is encrypted at rest according to industry standards.

11.5. Penetration testing and vulnerability scanning is conducted on the networks, applications and websites at appropriate periodic intervals.

11.6. The Supplier will provide details of the date the last tests were performed and evidence that any identified issues have been resolved.

11.7. Reviews of firewall and remote access logs are performed on a periodic basis.

11.8. Use of any media to record, store or process Sky personal data (including hard copy output, laptops, USB sticks, pen drives, CDs, or other magnetic media) is suitably authorised, handled, transported and encrypted.

12.Protection against Malicious Code

12.1. The Supplier shall apply and maintain operationally effective permanent controls on all relevant Supplier systems to prevent and detect the introduction of malicious software.

12.2. The supplier shall implement and maintain operationally effective detection and prevention measures and appropriate user awareness procedures

12.3. The Supplier shall promptly notify Sky as soon as it becomes aware of malicious code in systems directly affecting Sky personal data, and provide a report to Sky describing any incident and what measures were taken to prevent any reoccurrence.

13. System Management and User Access

13.1. The Supplier shall maintain systems security measures to guard against unauthorised access and system faults that could result in the loss or misuse of Sky personal data. As a minimum, the Supplier should have:

- a password and user account policy with which Supplier Personnel must comply which is aligned with industry best practice.
- controls over the data which a user can access and/or amend and ensure that appropriate authorisation has been granted before processing any change;
- controls to track the addition and deletion of users of the systems;
- controls to track user access to areas and functionality of the Systems;
- controls to ensure appropriate segregation of duties is maintained; and
- controls to ensure that access to systems containing Sky personal data is granted at the minimum level necessary.
- access privileges are amended or removed when business requirements or objectives change and leavers' accounts are removed promptly.

13.2. The Supplier shall ensure that any system faults where this affects systems used to process Sky personal data are logged, investigated, prioritised and rectified in timescales commensurate with the associated risks.

13.3. An automated system lock is to be invoked where a work station used to access or process Sky personal data is left unattended. The Supplier shall ensure that

restrictions on connection times shall be used to provide additional security for applications processing Tier 1 Sky personal data.

13.4. The Supplier shall, where applicable, ensure that all network access is subject to appropriate authentication and traffic controls and that all platform and application user accounts:

- are unique, justified, authorised, regularly reviewed;
- are granted the minimum required privileges to enable a user to perform their designated function;
- significant activity is logged and reviewed;
- access to audit trails is restricted and logged;
- default accounts are regularly deleted or disabled where possible and suitably authorised and controlled where this is not possible;
- privileged accounts, e.g. root, are only used when technically required under change control procedures and not for day-to-day system operation;
- where privileged account access is used, this access is logged and reviewed and access can be attributed to a named individual;
- access to databases is restricted - where assessed as critical, recent vulnerabilities are patched or mitigated; and
- access to information systems audit tools shall be restricted and controlled to prevent any possible misuse or compromise.

14. System Change Control

14.1. The Supplier shall apply a change control process which includes an assessment of security matters that may apply to any systems and which includes appropriate testing and rectification.

14.2. The Supplier shall ensure that production Sky personal data and information is not used for test purposes without the explicit written agreement of Sky.

14.3. The Supplier shall ensure that any new systems introduced into Sky's data environment are compliant with PCI DSS (where appropriate), the requirements of the relevant data protection law and other legal and regulatory requirements.

15. Platform and Application Security (where applicable to services)

The Supplier shall ensure that:

15.1. platforms and infrastructure used to transmit, collect, receive, process or store Sky personal data are built using consistent and formally documented platform build standards;

15.2. all unnecessary services are removed or disabled from platforms in accordance with the vendors' recommendations and active settings;

15.3. development, testing, production and operational facilities are separated both physically and logically to reduce the risks of unauthorised access or changes;

15.4. duties and responsibilities are segregated to reduce opportunities for unintentional or unauthorised misuse of Sky personal data;

15.5. appropriate patch management procedures are in place to remain current with platform security fixes, and conduct adequate testing;

15.6. all software installed on platforms used to receive, collect, store or process Sky personal data is authorised and fully licensed;

15.7. where cryptographic controls are implemented, they are securely managed using documented policy procedures, keys are subject to appropriate management and key changes are made under dual control and the impact of using encrypted information on controls that rely upon content inspection (e.g. malware detection) has been considered.

15.8. Where financial transactional functionality is (or becomes) a part of the Services provided by the Supplier to Sky, the Supplier shall provide data masking functionality in relation to bespoke software in respect of any financial data.

This section is applicable ONLY where the Supplier is providing application development and/or services from Supplier platforms:

15.9. The Supplier shall formally document and maintain technical security standards (including secure build configuration) for applications and systems used for Sky personal data.

15.10. The Supplier shall ensure that change control procedures are agreed and documented as regards the development of or implementation of or operation of bespoke systems used for Sky personal data and that such documented procedures include why the change was required and how and when the changes were executed.

15.11. The Supplier shall ensure that all new application developments, changes to existing systems, upgrades, and new software in relation to the Services have considered security control requirements, based upon the identified risks, and that all deliverables are tested and subject to an appropriate level of vulnerability scanning prior to being released to Sky, or being used as part of the services.

15.12. The Supplier shall ensure that application development is done in accordance with generally accepted good practice and that appropriate code review and validation controls are operated.

15.13. The Supplier shall ensure that access to and promotion of program source code is restricted and strictly controlled.

15.14. The Supplier shall ensure that back out procedures are documented prior to implementing any change or promoting a new piece of software.

16. Payment Card Industry Data Security Standards (where applicable to services)

Where payment card transactional functionality is (or becomes) a part of Services to Sky, the Supplier shall:

16.1. comply with the latest version under the PCI DSS requirements;

16.2. maintain a strategy for PCI DSS compliance in accordance with the Supplier's corporate information security policy which addresses each of the PCI DSS requirements and shall assign responsibility for PCI DSS to a designated person or compliance function;

16.3. provide evidence annually to Sky of PCI compliance through external certification

16.4. provide Sky with access to evidence that is used in supporting the Supplier's PCI compliance accreditation upon request and without undue delay.

16.5. ensure that a current network configuration diagram is produced and maintained to show clear data flows (including Sky's payment card transactions) and to ensure that all connections (including Sky's cardholder data) are identified including any wireless networks;

16.6. not disclose Sky cardholder data to any third party or entity with the exception of where this is authorised by Sky under the provision of Services to Sky or required by law;

16.7. maintain and provide on request a scope of the environment that is included in the assessment (e.g. Internet access points, internal corporate network) and identify any areas that are excluded from the PCI DSS Sky cardholder data environment;

16.8. maintain and provide on request details of any gap analysis that has been produced either internally or by a PCI DSS Qualified Security Advisor (QSA). This shall include details of the most recent Self-Assessment Questionnaire or Report on Compliance;

16.9. maintain and provide on request results of the most recent mandatory compliance or vulnerability scans as required by the PCI DSS;

16.10. maintain and provide on request details around any compensating controls to achieve risk mitigation in areas which do not meet the PCI DSS requirements; and

16.11. inform Sky immediately on any changes affecting the supplier's compliance status.

17.Customer Protection (where applicable to services)

17.1. Where Services involve the Supplier in direct interaction with Sky Customers, the Supplier provides ID passes for those personnel who will interact with the Customers, for example by visiting customers' premises.

17.2. The Supplier has a procedure in place for dealing with vulnerable customers.

Appendix 1 – Defined Terms

The following terms used herein shall have the following definitions:

"**Agreement**" means the agreement(s) between Sky and the Supplier which incorporates this Security Standard by inclusion or reference;

"**Customer**" – means the individuals or organisations who procure Services from Sky.

"**Data Controller**" – has the meaning ascribed to that term under the relevant data protection legislation from time to time;

"**Sensitive Data**" and "personal data" have the meaning set out in the Data Protection Act 1998 or any other equivalent;

"**Services**" – means the services provided by the Supplier to Sky as set out in the Agreement;

"**Sites**" - means any location utilised by the Supplier in providing the Services including but not limited to the Supplier's sites and any other location where Sky personal data is stored and/or processed.

"**Sky Data**" – means any and all data owned, processed or produced by or on behalf of Sky (including data produced by Supplier in the provision of the Services). This also includes any third-party data provided by Sky in the course of processing operations.

"**Sky Network**" means any electronic communications systems operated by the Sky group, namely Sky plc and any parent and all subsidiary undertakings from time to time or its affiliates or on their behalf;

"**Supplier**" – means organisations (and their Sky approved Sub-Contractors) that provide Services to Sky on a contractual basis;

"**Subcontractor**" – means contractor appointed by the Supplier in accordance with the Agreement to provide all or part of the Services;

"**Supplier Personnel**" means any employee, contractor or agent (including the employees of such contractor or agent) of the Supplier engaged by the Supplier to provide the Services;

"**Systems**" - means the information and communications technology system used by a party in performing the Services including any software, middleware, hardware, devices and peripheries.

Appendix 2 – Sky Account Criminal Record Guide

Never work on Sky Account	Consider work on Sky Account
Sexual offenders/on sexual offenders register	Civil offences (public order)
Drug related offences – supply and distribution Class A&B possession	Class C drug offences (possession only)
Violence/Assault/GBH/ABH	Motoring offences (depending on role)
Aggravated Theft/Burglary/handling stolen goods	Miscellaneous criminal convictions
Serious Fraud/white collar financial crime	
Firearms/weapon offences	
Harassment/stalking offences	
Miscellaneous petty theft offences	
Motoring offences (depending on role)	
Going equipped for stealing	
Blackmail	
Perjury	
Libel	
Obscene publication offences	

Appendix 3 – Adverse Financial Probity Guide

Disclosure	Action
Disclosed on Form	1. If less than £1,000 – NO ACTION (The CCJ must however be Satisfied (i.e., paid) or applicant provides proof that matter is being dealt with (e.g., paying £x per week). If not, applicant not to access Sky Customer Data until Satisfied or being dealt with. 2. If £1,000 + – obtain explanation and review. Note that CCJ and outstanding monies owed must be Satisfied or being dealt with, and non-multiple (i.e. 2 or less). If criteria met and satisfactory explanation received – NO ACTION. If not, applicant not to access Sky Customer Data until satisfied or being dealt with. If multiple CCJs the continued appointment must be risk assessed.
Not Disclosed on Form (The form used should leave the applicant in no doubt as to their requirements. A secondary level of guidance provided during induction & acknowledged by the applicant must remove any misunderstanding or ambiguity around what the applicant's obligations are)	Upon any disclosure, suspend, and investigate. Only where exceptional circumstances exist should NO ACTION be taken (e.g., it is believed the candidate had no knowledge of the court ruling). This aside the 'Not Disclosed' highlights a significant honesty and integrity issue and as such may not be considered suitable for appointment. If exceptional circumstances exist follow guidance above as if the candidate had 'Disclosed on Form'.

Appendix 4 – Supplier Levels

The data classification of suppliers is determined by the Sky Data Protection Office, in accordance with the applicable data protection legislation.

	Classification	Data Examples (not exhaustive)
Tier 1	**SECRET** Information which if lost or wrongly disclosed could cause very serious damage to the interests of Sky, our customers, people, suppliers and business partners	• Sensitive or Special categories of personal data, e.g. Racial origin, political opinion, religious belief • Bank account and payment card detail • Mother's Maiden name/PIN • Details of calls made and received • Content of Sky customer @sky.com email accounts
		• Secret business data • Bid processes • M&A projects • Price Sensitive information • Financial Statements (pre-release)
Tier 2	**CONFIDENTIAL** Personal information that can be traced to individual customers. Information which if lost or wrongly disclosed could cause distress to our customers or people, or damage the interests of Sky	• Personal data • Name/Address • Email/Telephone number • Age/DoB • Contacts with Sky (engineer visits) • Websites visited • Payment method/due date/collection • Viewing PIN • IP Address • Viewing card numbers
		• Confidential business data • System architecture • Performance reports • Project plans • Departmental budget information • Policies and standards • Newsletters • Non attributable data • Aggregate Customer information and viewing
Tier 3	**PUBLIC** No personally Identifiable Data held	• Data on public websites and social media • Data deemed to be public according to the applicable laws • • Data not able to identify the data subject • Forum postings • Product material – posters, flyers, adverts

Appendix 5 – Special provisions for Suppliers to Sky Deutschland

1. Clause 6.5 of this Security Standard is not applicable. Instead of this provision the following shall apply: If Sky personal data is to be accessed from outside the European Economic Area, there needs to be a written agreement in place between the Supplier and Sky, prior to the processing of such data. The agreement shall contain Standard Contractual Clauses or comparable provisions, i.e. binding corporate rules (as approved by the European Commission).

2. Clause 7.1 and appendices 2 and 3 are not applicable.

Appendix 6 – Special provisions for suppliers to Sky Italia

1. Clause 2.1. has to be amended to include the following:

"Accountability for data protection across all jurisdictions is clearly assigned by means of adequate written appointments to: (i) the individuals and/or entities supervising the data governance and data processing operations as Data Processors; (ii) the individuals (staff, etc) materially accessing personal data and/or carrying out processing operations as "persons in charge of the processing"; (iii) the individuals managing IT systems and relevant databases processing personal data as systems administrators."

2. The list of Supplier's obligations in Clause 6.1. has to be completed as follows:

- Authorization from Sky to the data disclosure to Supplier's Subcontractors;
- In case of an EU Supplier disclosing Sky data to extra-EU Subcontractors, formalization, between Sky and the Supplier, of a written representation proxy fulfilling the requirements under the Italian Civil Code is required. This proxy is the means of which the Supplier will enter, on behalf of Sky, into EU Standard Contractual Clauses with the Subcontractors;
- the appointment in writing of Subcontractors as data processors.

3. Clause 7.4, is to be amended to read as follows:

All Supplier Personnel are to sign an agreement and/or a letter of appointment as persons in charge of the processing, where applicable, which requires them to keep information confidential. This also covers Sky Data and/or Sky Materials.

4. Clause 8.4. is amended as follows:

Access to all entry points where Sky Data will be processed, including those at locations used by Subcontractors, is restricted and logged. System administrators' access logs (computer authentication) o the processing systems must be recorded in an unalterable format including timestamps and event descriptions for at least 6 months; the system administrators must be audited annually.

5. In Section 9, Clause 9.3 has to be added:

If the Supplier becomes or is made aware of any contravention of privacy or security requirements relating to the Sky personal data, or of unauthorised access to Sky Data, the Supplier shall:
- immediately report the incident to Cyber and Information Security Dept. at the following email address (incidentresponse@skytv.it) and to the Sky business relationship owner;
- promptly provide Sky with a written report setting out the details of the contravention of the data security requirements and describing any Sky Data which has or may have been compromised, measures taken by the Supplier or to be taken to minimize prejudice;
- provide Sky, at no additional cost, with all assistance required to restore the Sky Data and any other assistance that may be required by Sky;
- preserve evidence to include collection, retention and presentation to Sky Italia Cyber & Information Security;
- return to Sky any Sky Data;
- comply with all reasonable directions of Sky; and
- take immediate remedial action to secure the Sky Data and to prevent reoccurrences of the same or similar contravention and provide Sky with details of such remedial action.

6. Clause 11.2 will include the following additional points:

- Cookies (state how supplier adheres to applicable privacy law requirements as illustrated by ICO guidance);
- Adoption of security measures such as anonymization and pseudoanonimization, where appropriate, as well as all the security measures eventually set forth by the applicable local laws. Please remember that: (i) anti-virus must be daily updated, Network security (including firewall), anti-virus and patching must be updated at least monthly every 6 months; (ii) Removable storage media containing sensitive or judicial data must be destroyed after use, or re-used only if the data have been technically made unintelligible; (iii) For cookies, see par. 4.4 above.
- The keeping and updating the list of security measures and registers of the data processing operations, as well as ensuring that this requirement is fulfilled by the sub-processors themselves;
- Necessity of credentials management procedures (e.g. mandatory deactivation of credentials not used for at least six months);
- Passwords must be consistent with Sky Italia Information Security Policy requirements;
- At least annual verification of the authorization profiles.

7. Appendix 4 is to be amended to include the following additional data classification requirements:

- Where the data processed includes usage preferences, behavioral data or data processed for profiling purposes there are additional regulatory requirements in Italy such as prior approval by the regulator. Working with Sky, suppliers must evidence that these requirements have been met.
- Health data, biometrical data, video surveillance data as Secret Data;
- Pseudoanonimized data as Confidential Data.

Revision History

Date	Version	Summary of Changes
20/05/2011	V2.0	Refresh from previous release, including results of external review
30/06/2011	V2.1	Inclusion of Supplier levels at Appendix 4
08/07/2011	V2.2	Amendment of Subtitle – Change Management becomes System Change Control
30/08/2011	V2.3	Revision of content following input from DP team, IS Security and Company Secretariat
08/08/2012	V2.4	Annual legal review
28/01/2013	V2.5	V2.5 does not exist and was never created. The version control numbering has been changed to be concurrent with the PAWS online security checklist and both are now V2.6
28/01/2013	V2.6	Revision of content to subcontractor clauses to include audit requirements
September 2013	V2.7	Updated and revised post take over of process by ARMC – includes DP and IS Security review
October 2014	V2.8	Updated following annual review of the standard
February 2015	V2.9	Incorporation of Tier 1 and Tier 2 data standards and technical amendments to reflect best practice
February 2017	V3.0	Simplified into one standard. Draft for discussion.
February 2017	V3.1	Draft for discussion
March 2017	V3.2	Draft bringing in DE and IT comments
May 2017	V3.3	Final draft circulated to IS Security
June 2017	V3.5	Final Italian amends and IS Security minor changes. Sent to Procurement Legal.
July 2017	V3.6	Amends from Procurement Legal
July 2017	V4.0	Final for issue