



Sky Supplier Security Standard V4.1



**Sky Group Supplier
Security Standard v4.1**

October 2020



Sky Supplier Security Standard V4.1

Purpose

The Sky Security Standard (“SSS”) sets the minimum standards required of Suppliers to the Sky Group to meet appropriate technical and organisational measures for handling Sky Data, specifically Sky Personal Data.

“Sky Personal Data” for the purposes of this policy means any data relating to Sky staff, Sky customers or any other individuals where Sky is the Data Controller.

Data is only defined as Personal Data if it relates to an identifiable natural person who can be identified, directly or indirectly, by reference to the data in question. This document forms part of the Agreement entered into between a Supplier and Sky setting out the security obligations that Sky places on Suppliers.

The terms used in this standards document are defined in [Appendix 1](#).

The SSS is periodically reviewed and updated. The latest version is available at <https://www.skygroup.sky/corporate/about-sky/Suppliers> (latest Italian version can be found at eprocurement@sky.it)

Suppliers who are acting as Sky’s data processors will be required to demonstrate that they are operating appropriate technical and organisational measures and will be subject to regular review by Sky.

This review will take the form of either an independent audit, an on-site audit visit by Sky’s Risk, Controls and Assurance (“RCA”) team or by the Supplier’s completion of a questionnaire including supporting information.

The factors that will decide the type of review will include the volume and nature of personal data being handled, the impact on Sky and data subjects if it were lost, and the size and reputational risk of the supplier. Suppliers handling personal data will either be handling Tier 1 or Tier 2 data (or both). The nature of data in each Tier is set out in the table below.

Most suppliers handling only Tier 2 data will be reviewed remotely by the submission of a checklist but on-site visits by RCA will be considered on a rolling basis for those processing larger volumes or any with security concerns.

Suppliers handling large volumes of Tier 1 data, or based outside the EEA, or about whom there may be legitimate security concerns are likely to be subject to more rigorous audit procedures, which may include a request for an external audit. Other suppliers, handling smaller volumes of Tier 1 data, will not necessarily require an external audit.

The nature of the review that will be performed will be communicated to the Supplier by the Sky Business Relationship Owner.

Tier	Classification	Description / Examples (Personal Data)
1	Critical	Data the loss of which could cause significant distress and/or reputational or financial damage to individuals. This will normally include data which will enable third parties to identify individuals and which: <ul style="list-style-type: none">• is data about a person’s health, race, ethnicity, political views, religious or philosophical beliefs, trade union membership, genetic and biometric data, and data concerning a person’s sex life or sexual orientation – all of this data is classified as Special Category data in the GDPR;• relates to children; or• the loss or amendment of which or access to might cause particular distress to individuals – this includes specific financial information such as bank account or card numbers.



Sky Supplier Security Standard V4.1

2	Protected	Data the loss of which might cause distress to individuals but would be unlikely to cause them reputational or financial damage. This will normally include data which enable third parties to identify individuals, but which is neither Special Category data nor data about children nor specific financial information such as bank account or card numbers. Examples include: <ul style="list-style-type: none">• Name and other personal information such as age and date of birth,• Contact information such as postal address, email address, telephone numbers.
3	Not Protected	<ul style="list-style-type: none">• Personal Data which cannot lead to the identification of an individual by anyone outside Sky.

Territory Specific Provisions

Specific provisions apply to suppliers in Germany and Italy, as applicable, and are set out in Appendix 2 and Appendix 3 respectively.



Sky Security Standard

The Supplier shall demonstrate compliance with each of the below standards:

1. Policies and Codes of Conduct

- 1.1. Provide a copy of their employee code of conduct or similar document(s) covering anti-bribery and corruption, whistle-blowing and other appropriate ethics policies including anti-money laundering and anti-slavery.
- 1.2. Demonstrate these have been clearly communicated to all relevant staff.
- 1.3. Demonstrate 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, including details of the Data Protection Officer if applicable.
- 2.2. A clear data protection policy is in place and communicated to all relevant staff.
- 2.3. Processes are in place to ensure and demonstrate compliance with the data protection policy and any associated data governance policies.
- 2.4. 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 and such training is refreshed at regular intervals.
- 2.5. A process exists to ensure any messages containing Sky personal data are securely transmitted and sent only to the intended recipient.
- 2.6. 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. Sky can be notified of breaches via dp.department@sky.uk or, for Germany and Italy, at the email addresses in Appendices 2 and 3 respectively.
- 2.7. Sky will control the process of notifying individuals (Sky employees, customers or prospective customers) affected by the incident.
- 2.8. Confirmation should be provided by the Supplier to Sky that, to the best of their knowledge, there have been no unreported data breaches in the preceding 12-month period.
- 2.9. The Supplier maintains a central record of processing in accordance with local legislative requirements.
- 2.10. Processes are in place to record and maintain legitimate interest assessments, where applicable, to the legal basis of processing and a copy is available on request.
- 2.11. Processes are in place to conduct, document and maintain privacy impact assessments, where required, in accordance with local legislative requirements and a copy is available on request.

3. Data Collection, Retention and Destruction

- 3.1. 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.
- 3.2. The Supplier will adhere to the written agreed retention period for Sky personal data.
- 3.3. 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.
- 3.4. There are controls in place to ensure that the individual's chosen marketing preferences are adhered to.
- 3.5. Where web sites are used to collect Sky personal data and/or cookie data, this is done in accordance with the privacy notice displayed on the website and any other applicable privacy and cookie statements and/or consents in accordance with relevant legislation.



Sky Supplier Security Standard V4.1

- 3.6. There is a policy explaining how the Supplier uses personal data and cookies (if they are used) which is displayed to customers in accordance with relevant legislation.
- 3.7. The Supplier will obtain permission from Sky, in writing, 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.
- 3.8. 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.
- 3.9. The Supplier will ensure that all Sky data is destroyed in accordance with the Agreement on termination of Services and will provide evidence.

4. Subject Rights Requests

- 4.1. Where a subject request relating to Sky personal data is received by the Supplier, its Personnel are aware of how to identify it and know what to do when they receive such a request. The Supplier has a mechanism in place to respond to the request which includes notifying Sky, where relevant, within a timely period and in compliance with any regulatory requirements.
- 4.2. Where a subject request is received by Sky which is relevant to the Services provided by the Supplier, the Supplier has the requisite functionality on all systems which hold Sky personal data to comply within the appropriate time period agreed with Sky and in accordance with local legislative requirements.

5. Data Disclosure to Third Parties

- 5.1. Where Sky personal data will be processed by the Supplier's third parties, the Supplier will, except in cases where Sky has contractually authorized it to appoint sub-processors without further reference to Sky:
 - 5.1.1. Provide Sky with a list of all third parties with access to Sky personal data;
 - 5.1.2. Disclose what data will be accessible by them;
 - 5.1.3. Provide a list of countries where Sky personal data will be processed, including those outside of the European Economic Area ("EEA"). This includes, for example, outsourced data centres or cloud providers;
 - 5.1.4. Obtain authorisation from Sky to disclose Sky personal data to the third party;
 - 5.1.5. Consult or notify Sky, in writing, of any change in third party with access to Sky personal data; and
 - 5.1.6. Ensure written contracts or letters of appointment as data processors are in place between the Supplier and all such third parties to cover disclosure and data security requirements.
- 5.2. Where Sky personal data will be accessed from outside the European Economic Area there is a written agreement in place covering such processing. This agreement must include a recognised mechanism for a valid and lawful transfer outside the EEA, for example, the standard contractual clauses or binding corporate rules (as approved by the European Commission).
- 5.3. The Supplier has a contractual obligation to obtain assurance over the data security of all third parties with access to Sky personal data.
- 5.4. The Supplier conducts regular reviews of its third parties to ensure that they are taking appropriate technical and organisational measures to protect Sky personal data.
- 5.5. 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 and plans to rectify.
- 5.6. The Supplier maintains a register of relevant data protection breaches that have arisen at third parties.
- 5.7. All complaints relating to personal data are captured and recorded by the third party 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.

6. Personnel Security

- 6.1. Where appropriate to the nature and classification of Sky data accessed by the Supplier, the Supplier will conduct screening checks on its Personnel including reference checks and, where applicable, financial probity and criminal record checks, as appropriate to the job role and as permitted by local law.



Sky Supplier Security Standard V4.1

- 6.2. Where appropriate, these checks are refreshed on a periodic basis.
- 6.3. The results are logged and recorded.
- 6.4. All Supplier Personnel sign an agreement which requires them to keep information confidential including all Sky personal data.
- 6.5. 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.
- 6.6. Supplier Personnel are required to agree and adhere to all Supplier company policies, rules and procedures, including applicable data protection policies.
- 6.7. There is a clear process to handle Supplier Personnel who terminate their services with the Supplier including a policy to remove access to Sky Personal data from those Supplier Personnel within an appropriate timeframe.
- 6.8. 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.
- 6.9. The Supplier shall ensure its personnel is competent and adequately trained in information security necessary for the performance of the services.
- 6.10. The Supplier shall ensure that Sky personal data is only accessed by those who need such access in order to enable Supplier to discharge their obligations to Sky.

7. Physical and Environmental Security

- 7.1. 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.
- 7.2. The Supplier has a clearly defined physical security policy and related standards.
- 7.3. The requirements of the physical security policy are applied to all locations that will be used to support Sky operations.
- 7.4. Access to all entry points at all locations where Sky personal data will be processed is restricted, logged and reviewed.
- 7.5. 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.
- 7.6. 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.
- 7.7. The Supplier shall implement uninterruptible power supplies (“UPS”) for critical infrastructure and shall test the UPS regularly.
- 7.8. 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.
- 7.9. 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.
- 7.10. The Supplier shall ensure that prominent security signage or information detailing security policies and requirements are provided or displayed in all relevant locations, including electronically and on the Supplier’s intranet where one exists.
- 7.11. The Supplier will not perform the Services from locations other than those specified in the Agreement without obtaining the prior written consent of Sky, as far as reasonably possible. Any relocation will be implemented without causing disruption to the business of Sky or the provision of the Services
- 7.12. Where a shared Site is in operation, the Supplier shall:
 - 7.12.1. At 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
 - 7.12.2. 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.
- 7.13. A clear desk policy is operated at all Sites.
- 7.14. Organisational assets are protected by controls over the entire asset lifecycle from commissioning and deployment to removal and disposal.
- 7.15. Non-electronic information, for example data held in paper form, should be kept secure in appropriately locked storage facilities.
- 7.16. Supplier has a process to securely dispose of paper and printed material which may contain Sky personal data, such as faxes, email printouts, notes about customers or address labels.



8. Incident Response

- 8.1. The Supplier shall:
 - 8.1.1. Log all incidents with their origin and resolution; and
 - 8.1.2. Provide evidence relating to the security incident involving Sky personal data to Sky.
- 8.2. Sky can be notified of security incidents via dp.department@sky.uk or, for Germany and Italy, at the addresses set out in appendices 2 and 3 respectively.

9. Business Continuity and Disaster Recovery

- 9.1. The Supplier has 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.
- 9.2. The plans are tested annually or at such other agreed frequency.
- 9.3. Backups are taken and recovery is tested on a regular basis. Back-ups are encrypted and securely transported if taken off-site.
- 9.4. Capacity monitoring is in place for those systems that support the Supplier's provision of the Services to Sky.

10. Information Security

- 10.1. 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.
- 10.2. The Supplier's information security policy and the associated controls in operation should be regularly updated and reviewed and should include but are not limited to:
 - 10.2.1. Network and perimeter security;
 - 10.2.2. Protection of malicious code;
 - 10.2.3. Encryption (where applicable to services);
 - 10.2.4. Masking of personal data (for financial transactions); and
 - 10.2.5. Patching.
- 10.3. All Sky personal data is transferred or exchanged via secure channels which are appropriately encrypted according to industry standards.
- 10.4. All Sky personal data is encrypted at rest according to industry standards.
- 10.5. Penetration testing and vulnerability scanning is conducted on the networks, applications and websites at appropriate periodic intervals.
- 10.6. The Supplier will provide details of the date the last tests were performed and evidence that any identified issues have been resolved.
- 10.7. Reviews of firewall and remote access logs are performed on a periodic basis.
- 10.8. Use of any media to record, store, copy or Sky personal data (including hard copy output, laptops, USB sticks, pen drives, CDs, or other magnetic media) is restricted unless suitably authorised, handled, transported and encrypted.

11. Protection against Malicious Code

- 11.1. The Supplier shall apply and maintain operationally effective permanent controls on all relevant Supplier systems to prevent and detect the introduction of malicious software.
- 11.2. The Supplier shall implement and maintain operationally effective detection and prevention measures and appropriate user awareness procedures.



Sky Supplier Security Standard V4.1

- 11.3. 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.

12. System Management and User Access

- 12.1. 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:
- 12.1.1. A password and user account policy with which Supplier Personnel must comply which is aligned with industry best practice;
 - 12.1.2. Controls over the data which a user can access and/or amend and ensure that appropriate authorisation has been granted before processing any change;
 - 12.1.3. Controls to track the addition and deletion of users of the systems;
 - 12.1.4. Controls to track user access to areas and functionality of the Systems;
 - 12.1.5. Controls to ensure appropriate segregation of duties is maintained;
 - 12.1.6. Controls to ensure that access to systems containing Sky personal data is granted at the minimum level necessary;
 - 12.1.7. A process to amend or remove access privileges when business requirements or objectives change; and
 - 12.1.8. Leavers' accounts are removed promptly.
- 12.2. 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.
- 12.3. 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.
- 12.4. The Supplier shall, where applicable, ensure that all network access is subject to appropriate authentication and traffic controls:
- 12.4.1. All platform and application user accounts are unique, justified, authorised, regularly reviewed and are granted the minimum required privileges to enable a user to perform their designated function;
 - 12.4.2. Significant activity is logged and reviewed;
 - 12.4.3. Access to audit trails is restricted and logged;
 - 12.4.4. Default accounts are regularly deleted or disabled where possible and suitably authorised and controlled where this is not possible;
 - 12.4.5. Privileged accounts, e.g. root, are only used when technically required under change control procedures and not for day-to-day system operation;
 - 12.4.6. Where privileged account access is used, this access is logged and reviewed and access can be attributed to a named individual;
 - 12.4.7. Access to databases is restricted to authorised individuals; and
 - 12.4.8. Access to information systems audit tools shall be restricted and controlled to prevent any possible misuse or compromise.
- 12.5. Any mobile devices used for storing, processing or transmitting Sky data must be governed by a process which specifies:
- 12.5.1. Conditions for securing device access which may include for example PIN, ID or encryption;
 - 12.5.2. Controls over remote connections using Wifi or wireless data networks, teleworking or connection from public networks outside the Supplier's control; and
 - 12.5.3. Methods of remote administration including remote deletion of data.
- 12.6. Where Supplier personnel have access to systems administered by Sky:
- 12.6.1. Users must adhere to Sky policies on user administration and acceptable use;
 - 12.6.2. Connection must only be made through the method prescribed by Sky such as for example VPN;
 - 12.6.3. Suppliers must reconfirm all user access permissions when requested by Sky and at least every 6 months; and



Sky Supplier Security Standard V4.1

- 12.6.4. Suppliers must immediately notify Sky when an individual leaves the company or changes roles so that their access can be timely updated.

13. System Change Control

- 13.1. The Supplier shall apply a change control process which includes an assessment of any security issues before authorisation of a change into production environments detailing matters that may apply to any systems and which includes appropriate testing and rectification.
- 13.2. The Supplier shall ensure that production Sky personal data and information is not used for test purposes without the explicit written agreement of Sky.
- 13.3. 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.

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

- 14.1. The Supplier shall ensure that:
- 14.1.1. Platforms and infrastructure used to transmit, collect, receive, process or store Sky personal data are built using consistent and formally documented platform build standards;
 - 14.1.2. All unnecessary services are removed or disabled from platforms in accordance with the vendors' recommendations and active settings;
 - 14.1.3. Development, testing, production and operational facilities are separated both physically and logically to reduce the risks of unauthorised access or changes;
 - 14.1.4. Duties and responsibilities are segregated to reduce opportunities for unintentional or unauthorised misuse of Sky personal data;
 - 14.1.5. Appropriate patch management procedures are in place to remain current with platform security fixes, and conduct adequate testing;
 - 14.1.6. All software installed on platforms used to receive, collect, store or process Sky personal data is authorised and fully licensed;
 - 14.1.7. 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.
- 14.2. 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 related services (i.e. testing) from Supplier platforms:

- 14.3. The Supplier shall formally document and maintain technical security standards (including secure build configuration) for applications and systems used for Sky personal data.
- 14.4. The Supplier shall ensure that change control procedures are agreed and documented as regards the development, implementation 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.
- 14.5. 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.
- 14.6. 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.



Sky Supplier Security Standard V4.1

- 14.7. The Supplier shall ensure that access to, and promotion of, program source code is restricted, segregated and strictly controlled.
- 14.8. The Supplier shall ensure that back out procedures are documented prior to implementing any change or promoting a new piece of software.

15. 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:

- 15.1. Comply with the latest version of the PCI DSS requirements and provide evidence annually to Sky of PCI compliance through suitable external certification;
- 15.2. Provide Sky with access to evidence that is used in supporting the Supplier's PCI compliance accreditation upon request and without undue delay;
- 15.3. 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; and
- 15.4. Inform Sky immediately of any changes affecting the Supplier's compliance status.

16. Customer Protection (where applicable to services)

- 16.1. Where the Services involve the Supplier having direct interaction with Sky customers, for example by visiting customers' premises, the Supplier provides its Personnel with ID passes and ensures that its Personnel performing these roles are suitable to do so (in particular by reference to the provisions of clause 6.1 of this SSS)
- 16.2. The Supplier has a procedure in place for dealing with vulnerable customers or individuals.



Sky Supplier Security Standard V4

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;

“People” – means the individuals who work for Sky (including employees, interns, temporary/ contracted staff);

“Personal Data” and **“Special Category data”** have the meaning set out in the EU Regulation 2016/679 (GDPR) ;

“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, 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-processors) that provide Services to Sky on a contractual basis;

“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 peripherals.



Sky Supplier Security Standard V4.1

Appendix 2 – Special provisions for Suppliers to Sky Deutschland

1. Clause 6.1, 6.2, 6.3 are not applicable.
2. Clause 8.2 to add the following: Sky can be notified of security incidents via dsb@sky.de



Sky Supplier Security Standard V4.1

Appendix 3 – Special provisions for Suppliers to Sky Italia

1. Clause 2.1 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 Suppliers' obligations in Clause 3 and 4. to also include:

All suppliers have to certify compliance, before starting activities, with Cyber information. All Suppliers have to comply, and give evidence thereof, with Cyber information security and data protection requirements Policy (SKY-CIS-0352) as well with Cyber Security and Data Protection Checklist.
3. The list of Supplier's obligations in Clause 5.1. to also include:

5.1.7 In case of an EU Supplier disclosing Sky data to third parties outside the EU, formalisation, 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 by which the Supplier will enter, on behalf of Sky, into EU Standard Contractual Clauses or any other adequate measure with the third parties. In addition, a Data Transfer Impact Assessment must be completed by Supplier and sent back to Sky before any data transfers occur.

5.1.8 All Suppliers and sub-Suppliers have to comply, and give evidence thereof, with Cyber information security and data protection requirements Policy (SKY-CIS-0352) as well with Cyber Security and Data Protection Checklist.
4. Clause 6.4 is 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 including Sky Data.
5. Clause 7.4 shall be amended as follows:

Access to all entry points where Sky data will be processed, including those in places used by Sub-Processors, is limited and registered. System administrators' access logs (computer authentication) or processing systems must be recorded in an unalterable format, including time stamps and event descriptions for at least 6 months; system administrators must be audited annually.
6. In Section 8 the following clause is added:

8.2 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, and in any event within 24 hours, report the incident to the Data Protection Officer (legal.databreach@sky.it), to the Cyber and Information Security Department at the following email address incidentresponse@skytv.it and to the Sky business relationship owner.
 - promptly provide Sky with a written report containing details of the breach of data security obligations and a description of all Sky Data that has been or may have been compromised, the measures taken by the Supplier or to be taken to minimize damages;
 - provide Sky, at no additional cost, with all assistance necessary to restore the Sky Data and any other assistance that may be required by Sky;
 - retain evidence for collection, storage and presentation to Sky Italia's Cyber & Information Security Department;
 - return any Sky Data to Sky;



Sky Supplier Security Standard V4.1

- comply with all reasonable instructions from Sky; and
- take immediate corrective action to protect Sky data and prevent the recurrence of the same or similar violations and provide Sky with details of such corrective action.

7. Clause 10.2 shall be amended by adding the following:

- Cookies (indicate how the provider complies with applicable legal obligations regarding privacy as well as the requirements set out in the applicable measures and guidelines of the Data Protection Authority);
- Adoption of security measures such as anonymisation and pseudo-anonymisation, where appropriate, as well as any security measures that may be required by applicable local laws. Please note that: (i) Antivirus must be updated daily, network security (including firewall), antivirus and patches must be updated at least every 6 months; (ii) Removable storage devices containing sensitive/particular or judicial data must be destroyed after use or reused only if the data has been technically rendered unintelligible; (iii) For cookies, see par. above.
- Keeping and updating of the list of security measures and records of data processing operations, and consequent guarantee that this compliance is respected by the same sub-processors;
- Need for credential management procedures (e.g. mandatory deactivation of credentials not used for at least six months);
- Passwords must comply with the requirements of Sky Italia's Information Security Policy;
- At least one annual verification of authorization profiles.

8. Clause 12.4. is amended to also include:

12.4.9 System administrators' access to the processing systems must be logged and recorded in an unalterable format including timestamps and event descriptions for at least 6 months; the system administrators must be audited annually.