Overview of selected KPN Security Policies

Creation date: Wednesday, November 7, 2018 5:12:50 PM

Selected by: Ruud Leurs

Requirement	**Use of Traffic Data**
Description	Main rule: Traffic data must irreversible anonymized or deleted when it is no longer necessary for the transfer of communication or one of the exceptions stated below are applicable. Exception 1. Billing, traffic data may be used for billing purposes (this includes complaint handling, registration of prepaid credit, traffic management, information provision. Exception 2. Data retention. Traffic data must be kept for legal purposes. (6 months for telephony data and 3 months for internet data). Exception 3. Market analysis or sales activities. Traffic data may be used for market analysis or sales activities and added value services if and only if the customer has given prior permission (opt-in). Use of traffic data for market analysis or sales activities without prior permission is only possible if the traffic data is anonymized in an earlier stage.
Supplement	Without explicit permission of the customer (end-user) an traffic analysis is only allowed on anonymized data.
Related info	Clause 11.5 / 13.2a Telecom Act
ID	KSP-RE-633
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation

Requirement	**Regulations when deploying cameras**
Description	When deploying cameras within the Netherlands, KPN adheres to the data protection act (AVG).
ID	KSP-RE-615
Version	1.1
Internal use	Yes, internal use only
Date	November 2, 2018
Rationale	Law and regulation
Rationale	Physical security

<table>
<tr><td>Requirement</td><td>Retention period</td></tr>
<tr><td>Description</td><td>Images may not be retained longer than specified below:

<table>
<tr><th colspan="3">Maximum permitted storage of CCTV-recordings</th></tr>
<tr><th>Name</th><th>Calendar days</th><th>Ad</th></tr>
<tr><td>KPN Retail</td><td>28</td><td>(1)</td></tr>
<tr><td>KPN Other</td><td>28</td><td>(1)</td></tr>
<tr><td>KPN International Germany</td><td>10</td><td>(2)</td></tr>
<tr><td>KPN International Other</td><td>28</td><td>(2)</td></tr>
<tr><td>Monitoring on behalf of Ministry of Justice</td><td>183</td><td>(3)</td></tr>
<tr><td colspan="3">NB: No audio recording without authorization of the CSO</td></tr>
</table>

Ad (1)

According to the KPN Camera use policy the standard maximum permitted storage of CCTV-images is 28 calendar days.

Ad (2)

All the CCTV-images will we stored based on motion detection. The maximum permitted storage of CCTV-images for KPN International is 28 calendar days. Only in Germany is the maximum permitted storage of CCTV-images 10 days.

Ad (3)

The maximum permitted storage of 183 calender days on behalf of the Ministry of Justice is originated from #de regeling BBGT#

The CSO may decide to retain images for a longer period if an investigation so requires.</td></tr>
<tr><td>ID</td><td>KSP-RE-616</td></tr>
<tr><td>Version</td><td>1.0</td></tr>
<tr><td>Internal use</td><td>Yes, internal use only</td></tr>
<tr><td>Date</td><td>December 11, 2017</td></tr>
<tr><td>Rationale</td><td>Law and regulation</td></tr>
<tr><td>Rationale</td><td>Physical security</td></tr>
</table>

Requirement	Notification
Description	Wherever camera monitoring is deployed and the images are stored, the public has to be notified by means of a pictogram/sign or an appropriate text.
ID	KSP-RE-617
Version	1.0
Internal use	Yes, internal use only
Date	December 11, 2017
Rationale	Law and regulation
Rationale	Physical security

Requirement	**Continuity Incident Reporting**
Description	Major incidents in Telecom Act relevant services with severe continuity impact (Code Orange or Code Red) must be reported to authority as part of the established Be Alert process.
Supplement	Providers of public electronic communications networks and public electronic communications services inform the Minister without delay of: a. a security breach b. a loss of integrity allowing the continuity of public electronic communications networks and public electronic communications significantly interrupted.
Related info	Article 11a.2 of the Dutch Telecommunications Law [NL only]
ID	KSP-RE-660
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation

Requirement	**External Compliance Reporting**
Description	KPN CISO reports the status to relevant authorities (Agentschap Telecom) at their request.
Supplement	Providers of public electronic communications networks and public electronic communications provide our Minister at his request, any information necessary to assess the safety and integrity of their networks and services.
Related info	Article 11a.2, section 2, of the Dutch Telecommunications Law [NL only]
ID	KSP-RE-661
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation

Requirement	**Exceptional circumstances**
Description	Instructions government under exceptional circumstances.
Supplement	The government can give instructions under exceptional circumstance for: a. the availability of public telecommunications networks or parts of it, public telecommunications and radio transmission equipment; b. the protection of certain parts of a public telecommunications network or radio transmission equipment; c. the settlement of the electronic transport of data over a public telecommunications network, and d. Additional infrastructure for the electronic transmission of data and the security. The measures and contingency plans for this are addressed in subject area Business Continuity, whereby the additional requirements with respect to KPN Critical Services and NL Vital Services are especially important. Corporate Crisis Management is in place to manage the situation on strategic level as Be Alert code Red, with control of the Be Alert code Orange teams for operational tasks.
Related info	Article 14 of the Dutch Telecommunications Law (14.1-14.6) [NL only]
ID	KSP-RE-662
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation

Requirement	Responsible employee
Description	KPN CISO is responsible to manage that BCM policies are defined and that reporting units are working up to, and reporting the level of compliancy to these policies.
Supplement	This complies with Article 2, paragraph 1 b, of the Decree continuity public electronic communications networks and services : the designation of a skilled officer who is responsible and available within his organization to take and implement the measures.
Related info	Article 2 of the Dutch ‘Decree continuity public electronic communications networks and services’ [NL only]
ID	KSP-RE-658
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation
Rationale	Determine BCM planning & process
Rationale	Implementing changes

Requirement	**Continuity Plan**
Description	KPN must create and maintain a Continuity Plan.
Supplement	This meets the relevant requirements from the Telecommunications Law and the Decree continuity public electronic communications networks and services: Providers of public electronic communications networks and public electronic communications services take appropriate technical and organizational measures to appropriately manage the risks to the safety and integrity of their networks and services.
Related info	http://wetten.overheid.nl/BWBR0009950/Hoofdstuk11a/Artikel11a1/geldigheidsdatum_24-06-2015 http://wetten.overheid.nl/BWBR0032149/geldigheidsdatum_23-09-2013#i2_Artikel2
ID	KSP-RE-659
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation
Rationale	Determine BCM planning & process
Rationale	Implementing changes

Requirement	**Reporting Incidents**
Description	Be Alert incidents with orange or red classification on Telecom Law relevant services must be registered by SQC to AT website within 24 hours and to CISO. When needed follow-up messages must be registered when classification changes or when updates are available.
ID	KSP-RE-618
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation

Requirement	**Processing of personal data by third parties on behalf of KPN**
Description	When personal data is processed by a third party a specific data processor agreement is mandatory (for example EU Model Clause).
Supplement	Mandatory (European) legal rules, Countries in the European Economic Area (EEA) are required to have a similar standard of protection of personal data but this is not always the case in countries outside of the EEA. When a contract is closed, in which a third party processes personal- or traffic data, a signed EU Model Clause is mandatory.
Related info	Directive 95/46/EC and clause 77 section 1 g Wet bescherming persoonsgegevens. This document is available on a secure portal for Purchase Office employees.
ID	KSP-RE-632
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation

Requirement	**Retention periods**
Description	Data must be stored in accordance with legal retention periods.
Supplement	Internet traffic data may only be stored for a period of maximum 6 months.
Related info	See “Juridisch Doe-Het-Zelf“ on TEAMKPN
ID	KSP-RE-631
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation

Requirement	**Use of Personal Data**
Description	KPN may only use data for: - To (technically) deliver the services; - The management of the relationship between KPN and the customer, including all activities related to the preparation and execution of the agreements concluded between KPN and the customer; - Management of the relationship with the customer, including note inquiry, complaint handling, noise removal, consulting; - The billing process including billing for prepaid and MMS-services including note inquiry, complaint handling, consulting; - Network management, including network management, network planning, network architecture, network integrity and fraud detection and promote continuity; - Processing for a business operations, including security, expansion and improvement of the network and the services; - Comply with legal obligations, if the provision of information in the context of a criminal investigation; - Provision of personal data to third parties for the purpose of issuing (electronic) telephone directories; - The processing of personal data (also after termination of contract) for market research, marketing, sales or service of KPN products
Supplement	Processing of customer data is only allowed in accordance with the agreement (privacy statement) see also requirement KSP-RE-640.
Related info	Wet bescherming persoonsgegevens Privacy Statement van KPN
ID	KSP-RE-634
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation

Requirement	**Safeguarding of Personal Data by taking information security measures**
Description	KPN must take all necessary technical and organizational measures to ensure the safety and security of networks and services offered. This results in the protection of personal data against loss or any form of unlawful processing. These measures guarantee a level of security appropriate to the risks represented by the processing and the nature of data to be protected. The measures are also aimed at unnecessary collection and further processing of personal data.
Supplement	Personal data needs to be protected according to the data protection act (AVG), elaboration of the measures are published on the data protection authority ('Autoriteit Persoonsgegevens') website. In case of an incident the 'Autoriteit Persoonsgegevens' (AP) will revert to their issued standards and guidelines. It is strongly advised to determine any deviations between the KPN information security policy and the AP guidelines and align KPN's information security policy with these guidelines. A risk analysis (Data Protection Impact Assessment) needs to be performed at least once a year. A penetration test is mandatory before a new portal is released.
Related info	Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" (October 2017): https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20171013_wp248_rev01_enpdf.pdf Clause 11a.1 Telecommunicatiewet Internal Control Framework (GRC+) This requirement is addressed through the entire KSP (KPN Security Policy framework) which has the objective to take appropriate technical and organizational measures.
ID	KSP-RE-635
Version	1.1
Date	November 2, 2018
Rationale	Law and regulation

Requirement	**Information security breach and notification**
Description	KPN must report a violation related to personal data to Autoriteit Persoonsgegevens (AP) and to the affected end users without unnecessary delays but in any case within 24 hours and take action to remedy the infringement as soon as possible. Compliance incidents must be reported to the KPN Helpdesk Security, Compliance & Integrity as soon as possible. The KPN Helpdesk Security, Compliance & Integrity and the department Risk & Compliance are responsible for reporting to the AP.
Related info	Clause 11.3a Telecom Act
ID	KSP-RE-636
Version	1.2
Date	November 2, 2018
Rationale	Law and regulation

Requirement	**Storage and destruction of customer data**
Description	KPN must ensure that personal data is always secure, commissioned by KPN and under secrecy by a processor. Furthermore personal data shall only be kept (in a form which permits identification of the data subject) for as long as necessary for achieving the purposes for which they are collected and/or further processed.
Related info	Chapter 11 and 13 Telecom Act and clause 10 Wet bescherming persoonsgegevens
ID	KSP-RE-637
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation

Requirement	**SPAM (unsolicited approaches)**
Description	KPN only approaches users with unsolicited commercial communications if they have not objected and are not listed in the “call-me-not” register.
Related info	Clause 11.7, 11.8 Telecom Act
ID	KSP-RE-638
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation

Requirement	**Cookies**
Description	Customers must be informed when Cookies are used which have an impact on privacy, these cookies (such as tracking cookies) , may only be used with the consent of the customer.
Supplement	Mandatory legal obligation. From a privacy point of view there are two types of cookies. Cookies with minor consequences for the privacy and cookies which have consequences for the privacy. For cookies with minor consequences (as analytical cookies, a/b testing cookies and affiliate cookies) no permission is required.
Related info	Clause 11.7a Telecom Act
ID	KSP-RE-639
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation

Requirement	**Opt-in and Opt-out**
Description	KPN has a legitimate interest in processing customer data for (direct) marketing and analysis. A trade-off should be made between the interest of KPN and the privacy of the customer. If the information is less sensitive the balance is in favour of KPN. KPN may use this information, but the customer must have an opportunity to object (hence opt-out). If the information is more sensitive they can only be used with the prior permission of the customer (hence opt-in). Examples of less sensitive data are customer registration data, installed base, product/service usage. Examples of more sensitive data are traffic data or data regarding online behaviour.
Supplement	An analysis of mobile traffic data for marketing purposes may only be made with prior permission of the customer.
Related info	See factsheet Customer Privacy – Opt-in / Opt-out Compliancy Beleid http://teamkpn.kpn.org/group/kpninfo-read/groep-juridisch-doe-het-zelf/pS_T9DOv9QKXINVQTtBaRB2wsGtqMnl7_v-yxpjqZk0H_CmybaW2BA**/
ID	KSP-RE-640
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation

Requirement	**Right to access personal data**
Description	KPN must give access to the personal data stored of a person upon a request of that person.
Related info	Clause 35 Wet bescherming persoonsgegevens http://www.kpn.com/privacy.htm under no. 7
ID	KSP-RE-641
Version	1.0
Date	December 11, 2017
Rationale	Law and regulation

Requirement	**Right to correct personal data**
Description	The right to correction includes the right to ask questions to improve, supplement, remove or blocking of personal data. A customer shall have the right to correction requests in three cases: 1. The personal data are factually incorrect; 2. The personal data for the purpose or purposes for which it is collected are incomplete or irrelevant; 3. The personally identifiable information is used in a different way in violation of any law.
Related info	Clause 36 Wet bescherming persoonsgegevens and eighth item of the Privacy Statement of KPN
ID	KSP-RE-642
Version	1.1
Date	April 4, 2018
Rationale	Law and regulation