

Friday, April 20, 2018 10:11:55 AM

Ruud Leurs

Requirement	Use of Traffic Data
<b>Description</b>	<p>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.</p> <p>Exception 1. Billing, traffic data may be used for billing purposes (this includes complaint handling, registration of prepaid credit, traffic management, information provision.</p> <p>Exception 2. Data retention. Traffic data must be kept for legal purposes. (6 months for telephony data and 3 months for internet data).</p> <p>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.</p>
<b>Supplement</b>	Without explicit permission of the customer (end-user) an traffic analysis is only allowed on anonymized data.
<b>Related info</b>	Clause 11.5 / 13.2a Telecom Act
<b>ID</b>	KSP-RE-633
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Law and regulation

<b>Requirement</b>	<b>Regulations</b>
<b>Description</b>	When deploying cameras within the Netherlands, KPN adheres to the Dutch Data Protection Act (Wbp).
<b>ID</b>	KSP-RE-615
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Law and regulation
<b>Rationale</b>	Physical security

Requirement	Retention period																					
Description	<p>Images may not be retained longer than specified below:</p> <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></table> <p>NB: No audio recording without authorization of the CSO</p> <p>Ad (1)</p> <p>According to the KPN Camera use policy the standard maximum permitted storage of CCTV-images is 28 calendar days.</p> <p>Ad (2)</p> <p>All the CCTV-images will be 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.</p> <p>Ad (3)</p> <p>The maximum permitted storage of 183 calendar days on behalf of the Ministry of Justice is originated from #de regeling BBGT#</p> <p>The CSO may decide to retain images for a longer period if an investigation so requires.</p>	Maximum permitted storage of CCTV-recordings			Name	Calendar days	Ad	KPN Retail	28	(1)	KPN Other	28	(1)	KPN International Germany	10	(2)	KPN International Other	28	(2)	Monitoring on behalf of Ministry of Justice	183	(3)
Maximum permitted storage of CCTV-recordings																						
Name	Calendar days	Ad																				
KPN Retail	28	(1)																				
KPN Other	28	(1)																				
KPN International Germany	10	(2)																				
KPN International Other	28	(2)																				
Monitoring on behalf of Ministry of Justice	183	(3)																				
ID	KSP-RE-616																					
Version	1.0																					
Date	December 11, 2017																					
Rationale	Law and regulation																					

<b>Rationale</b>	Physical security
------------------	-------------------

<b>Requirement</b>	<b>Notification</b>
<b>Description</b>	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.
<b>ID</b>	KSP-RE-617
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Law and regulation
<b>Rationale</b>	Physical security

<b>Requirement</b>	<b>Continuity Incident Reporting</b>
<b>Description</b>	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.
<b>Supplement</b>	<p>Providers of public electronic communications networks and public electronic communications services inform the Minister without delay of:</p> <ul style="list-style-type: none"> <li>a. a security breach</li> <li>b. a loss of integrity</li> </ul> <p>allowing the continuity of public electronic communications networks and public electronic communications significantly interrupted.</p>
<b>Related info</b>	Article 11a.2 of the Dutch Telecommunications Law [NL only]
<b>ID</b>	KSP-RE-660
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Law and regulation

<b>Requirement</b>	<b>External Compliance Reporting</b>
<b>Description</b>	KPN CISO reports the status to relevant authorities (Agentschap Telecom) at their request.
<b>Supplement</b>	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.
<b>Related info</b>	Article 11a.2, section 2, of the Dutch Telecommunications Law [NL only]
<b>ID</b>	KSP-RE-661
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Law and regulation



Requirement	Exceptional circumstances
Description	Instructions government under exceptional circumstances.
Supplement	<p>The government can give instructions under exceptional circumstance for:</p> <ul style="list-style-type: none"> <li>a. the availability of public telecommunications networks or parts of it, public telecommunications and radio transmission equipment;</li> <li>b. the protection of certain parts of a public telecommunications network or radio transmission equipment;</li> <li>c. the settlement of the electronic transport of data over a public telecommunications network, and</li> <li>d. Additional infrastructure for the electronic transmission of data and the security.</li> </ul> <p>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.</p> <p>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.</p>
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	<p>This complies with Article 2, paragraph 1 b, of the Decree continuity public electronic communications networks and services :</p> <p>the designation of a skilled officer who is responsible and available within his organization to take and implement the measures.</p>
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

<b>Requirement</b>	<b>Continuity Plan</b>
<b>Description</b>	KPN must create and maintain a Continuity Plan.
<b>Supplement</b>	<p>This meets the relevant requirements from the Telecommunications Law and the Decree continuity public electronic communications networks and services:</p> <p>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.</p>
<b>Related info</b>	<p><a href="http://wetten.overheid.nl/BWBR0009950/Hoofdstuk11a/Artikel11a1/geldigheidsdatum_24-06-2015">http://wetten.overheid.nl/BWBR0009950/Hoofdstuk11a/Artikel11a1/geldigheidsdatum_24-06-2015</a></p> <p><a href="http://wetten.overheid.nl/BWBR0032149/geldigheidsdatum_23-09-2013#i2_Artikel2">http://wetten.overheid.nl/BWBR0032149/geldigheidsdatum_23-09-2013#i2_Artikel2</a></p>
<b>ID</b>	KSP-RE-659
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Law and regulation
<b>Rationale</b>	Determine BCM planning & process
<b>Rationale</b>	Implementing changes

<b>Requirement</b>	<b>Reporting Incidents</b>
<b>Description</b>	<p>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.</p> <p>When needed follow-up messages must be registered when classification changes or when updates are available.</p>
<b>ID</b>	KSP-RE-618
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Law and regulation

<b>Requirement</b>	<b>Processing of personal data by third parties on behalf of KPN</b>
<b>Description</b>	When personal data is processed by a third party a specific data processor agreement is mandatory (for example EU Model Clause ).
<b>Supplement</b>	<p>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.</p> <p>When a contract is closed, in which a third party processes personal- or traffic data, a signed EU Model Clause is mandatory.</p>
<b>Related info</b>	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.
<b>ID</b>	KSP-RE-632
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Law and regulation

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

Requirement	Use of Personal Data
Description	<p>KPN may only use data for:</p> <ul style="list-style-type: none"> <li>- To (technically) deliver the services;</li> <li>- 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;</li> <li>- Management of the relationship with the customer, including note inquiry, complaint handling, noise removal, consulting;</li> <li>- The billing process including billing for prepaid and MMS-services including note inquiry, complaint handling, consulting;</li> <li>- Network management, including network management, network planning, network architecture, network integrity and fraud detection and promote continuity;</li> <li>- Processing for a business operations, including security, expansion and improvement of the network and the services;</li> <li>- Comply with legal obligations, if the provision of information in the context of a criminal investigation;</li> <li>- Provision of personal data to third parties for the purpose of issuing (electronic) telephone directories;</li> <li>- The processing of personal data (also after termination of contract) for market research, marketing, sales or service of KPN products</li> </ul>
Supplement	Processing of customer data is only allowed in accordance with the agreement (privacy statement) see also requirement KSP-RE-640.
Related info	<p>Wet bescherming persoonsgegevens</p> <p>Privacy Statement van KPN</p>
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
<b>Description</b>	<p>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.</p> <p>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.</p>
<b>Supplement</b>	<p>Personal data needs to be protected according to the “Wet bescherming persoonsgegevens”, elaboration of the measures are published in the “CBP Richtsnoeren, beveiliging van persoonsgegevens”.</p> <p>In case of incident(s) CBP will revert to their issued standards and guidelines. It is strongly advised to determine any deviations between KPN information security policy and the CBP guidelines and align KPN’s information security policy with the guidelines.</p> <p>A risk analysis needs to be performed at least once a year.</p> <p>A penetration test is mandatory before a new portal is released.</p>
<b>Related info</b>	<p>Clause 13 Wet bescherming persoonsgegevens</p> <p>Clause 11a.1 Telecommunicatiewet</p> <p>Internal Control Framework (GRC+)</p> <p>This requirement is addressed through the entire KSP (KPN Security Policy framework) which has the objective to take appropriate technical and organizational measures.</p> <p>Richtsnoeren beveiliging persoonsgegevens, CBP (febr. 2013)</p> <p><a href="http://www.cbweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx">http://www.cbweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx</a></p>
<b>ID</b>	KSP-RE-635
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Law and regulation



<b>Requirement</b>	<b>Information security breach and notification</b>
<b>Description</b>	<p>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.</p> <p>Compliance incidents must be reported to the KPN Helpdesk Security, Compliance &amp; Integrity as soon as possible. The KPN Helpdesk Security, Compliance &amp; Integrity and the department Corporate Compliance are responsible for reporting to the AP.</p>
<b>Related info</b>	Clause 11.3a Telecom Act
<b>ID</b>	KSP-RE-636
<b>Version</b>	1.1
<b>Date</b>	April 4, 2018
<b>Rationale</b>	Law and regulation

<b>Requirement</b>	<b>Storage and destruction of customer data</b>
<b>Description</b>	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.
<b>Related info</b>	Chapter 11 and 13 Telecom Act and clause 10 Wet bescherming persoonsgegevens
<b>ID</b>	KSP-RE-637
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Law and regulation

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

<b>Requirement</b>	<b>Cookies</b>
<b>Description</b>	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.
<b>Supplement</b>	<p>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.</p> <p>For cookies with minor consequences (as analytical cookies, a/b testing cookies and affiliate cookies) no permission is required.</p>
<b>Related info</b>	Clause 11.7a Telecom Act
<b>ID</b>	KSP-RE-639
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Law and regulation

Requirement	Opt-in and Opt-out
<b>Description</b>	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.
<b>Supplement</b>	An analysis of mobile traffic data for marketing purposes may only be made with prior permission of the customer.
<b>Related info</b>	See factsheet Customer Privacy – Opt-in / Opt-out Compliancy Beleid  <a href="http://teamkpn.kpn.org/group/kpninfo-read/groep-juridisch-doe-het-zelf/pS_T9DOv9QKXINVQTtBaRB2wsGtqMnl7_v-yxpjqZk0H_CmybaW2BA**/">http://teamkpn.kpn.org/group/kpninfo-read/groep-juridisch-doe-het-zelf/pS_T9DOv9QKXINVQTtBaRB2wsGtqMnl7_v-yxpjqZk0H_CmybaW2BA**/</a>
<b>ID</b>	KSP-RE-640
<b>Version</b>	1.0
<b>Date</b>	December 11, 2017
<b>Rationale</b>	Law and regulation

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

<b>Requirement</b>	<b>Right to correct personal data</b>
<b>Description</b>	<p>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:</p> <ol style="list-style-type: none"> <li>1. The personal data are factually incorrect;</li> <li>2. The personal data for the purpose or purposes for which it is collected are incomplete or irrelevant;</li> <li>3. The personally identifiable information is used in a different way in violation of any law.</li> </ol>
<b>Related info</b>	Clause 36 Wet bescherming persoonsgegevens and eighth item of the Privacy Statement of KPN
<b>ID</b>	KSP-RE-642
<b>Version</b>	1.1
<b>Date</b>	April 4, 2018
<b>Rationale</b>	Law and regulation