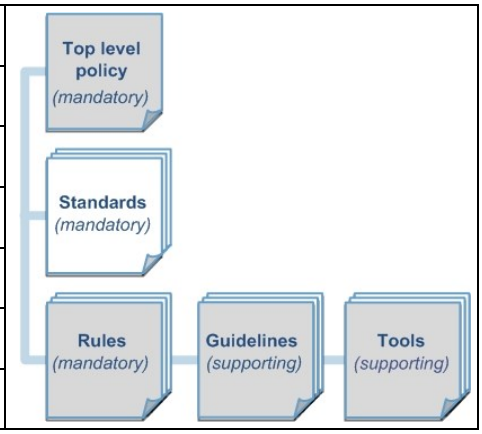
KPN Security Policy

KSP – Standard

Title	**Privacy and Personal Data Protection**
ID	**KSP-FA10-ST01**
Funct. Area	FA10 – Regulatory Requirements
Date	29 April 2016
Version	v1.7
Status	Approved
Owner	Privacy Officer



Summary

Due to the nature of its services KPN processes personal- and traffic data from its customers. KPN needs to ensure that this data is carefully handled and makes sure that every processing of such data complies with the applicable laws and regulations.

ID	KSP-FA10-ST01-R01
Title	Retention periods
Description	Data must be stored in accordance with legal retention periods.
Relating document	See “Juridisch Doe-Het-Zelf“ on TEAMKPN
Rationale (why)	Mandatory legal obligations from different legislations.
Example	Internet traffic data may only be stored for a period of maximum 6 months.
Possible exception	N/A

ID	KSP-FA10-ST01-R02
Title	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).
Relating document	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.
Rationale (why)	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.
Example	When a contract is closed, in which a third party processes personal- or traffic data, a signed EU Model Clause is mandatory.
Possible exception	N/A

ID	KSP-FA10-ST01-R03
Title	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.
Relating document	Clause 11.5 / 13.2a Telecom Act
Rationale (why)	Mandatory legal rules.
Example	Without explicit permission of the customer (end-user) an traffic analysis is only allowed on anonymized data.
Possible exception	N/A

ID	KSP-FA10-ST01-R04
Title	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
Relating document	http://wetten.overheid.nl/BWBR0011468/ http://www.kpn.com/privacy.htm
Rationale (why)	Mandatory legal rules.
Example	Processing of customer data is only allowed in accordance with the agreement (privacy statement) see also requirement KSP-FA10-ST01-R10.
Possible exception	N/A

ID	KSP-FA10-ST01-R05
Title	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.
Relating document	Clause 13 Wet bescherming persoonsgegevens 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. Richtsnoeren beveiliging persoonsgegevens, CBP (febr. 2013) http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx
Rationale (why)	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”. 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.
Example	A risk analysis needs to be performed at least once a year. A penetration test is mandatory before a new portal is released.
Possible exception	N/A

ID	KSP-FA10-ST01-R06
Title	Information security breach and notification
Description	KPN must report a violation related to personal data to Autoriteit Persoonsgegevens (AP) within 24 clock hours and to the affected end users and takes 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 Corporate Compliance are responsible for reporting to the AP.
Relating document	Clause 11.3a Telecom Act
Rationale (why)	Mandatory legal obligation.
Example	N/A
Possible exception	N/A

ID	KSP-FA10-ST01-R07
Title	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.
Relating document	Chapter 11 and 13 Telecom Act and clause 10 Wet bescherming persoonsgegevens
Rationale (why)	Mandatory legal obligation.
Example	N/A
Possible exception	N/A

ID	KSP-FA10-ST01-R08
Title	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.
Relating document	Clause 11.7, 11.8 Telecom Act
Rationale (why)	Mandatory legal obligation.
Example	N/A
Possible exception	N/A

ID	KSP-FA10-ST01-R09
Title	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.
Relating document	Clause 11.7a Telecom Act
Rationale (why)	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.
Example	N/A
Possible exception	N/A

ID	KSP-FA10-ST01-R10
Title	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.
Relating document	See factsheet Customer Privacy – Opt-in / Opt-out Compliancy Beleid
Rationale (why)	Clause 8, 41.1 Wet bescherming persoonsgegevens.
Example	An analysis of mobile traffic data for marketing purposes may only be made with prior permission of the customer.
Possible exception	N/A

ID	KSP-FA10-ST01-R11
Title	Right to access personal data
Description	KPN must give access to the personal data stored of a person upon a request of that person.
Relating document	Clause 35 Wet bescherming persoonsgegevens http://www.kpn.com/privacy.htm under no. 7
Rationale (why)	Mandatory legal obligation.
Example	N/A
Possible exception	N/A

ID	KSP-FA10-ST01-R12
Title	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.
Relating document	Clause 36 Wet bescherming persoonsgegevens http://www.kpn.com/privacy.htm under no. 8
Rationale (why)	Mandatory legal obligation.
Example	N/A
Possible exception	N/A