Overview of selected
KPN Security Policies

Creation date: Thursday, May 9, 2019 3:17:47 PM

Selected by: Ruud Leurs

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	**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	**Identity Management Systems**
Description	Identity Management systems (and chains of systems), such as (but not limited to) Active Directory Servers, Kerberos Servers, Identity & Access Management systems must be located within KPN premises and maintained by KPN (EP) employees.
Supplement	KPN must be in ultimate control of who can access information of KPN's customers and KPN. An application owner must be able to grant or deny access to the information systems under his control, without possible intervention by third parties.
ID	KSP-RE-375
Version	1.0
Date	December 11, 2017
Rationale	Central identity and access management

Requirement	Encryption Algorithms
Description	One of the following encryption primitives must be used for encryption and decryption: AES-256, AES-192 and AES-128 XSalsa20/20 Salsa20/20 Camellia Twofish IDEA; the key must be generated using a hash algorithm from KSP-RE-483, like SHA2 For AES and Camellia use known good authenticated modes: GCM CCM Use non-authenticated cipher modes only in combination with an authentication method, like HMAC: CTR XTS The following encryption primitives should not be used. Use only for legacy support or explicit compatibility requirements: AES-256-CBC, AES-192-CBC and AES-128-CBC in combination with TLSv1.0 Camellia-CBC in combination with TLSv1.0 Three-key Triple DES Blowfish All not explicitly mentioned encryption algorithms are not allowed. Example are: RC4 All EXPORT ciphers All encryption algorithms resulting in less than 112 security bits The use of a random nonce or initialisation vector (IV) with sufficient length is mandatory with each of these encryption algorithms. To generate a good nonce or IV use a good random bit generator.

Related info	NIST Special Publication 800-131Ar1: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
ID	KSP-RE-479
Version	1.2
Date	February 1, 2019
Rationale	Cryptography generic

Requirement	**Pseudonymization**
Description	Personal data must be stripped from directly identifying characteristics by using hashing.
Supplement	Personal data must be processed in such a way, that the identifiable personal information is encrypted. People may no longer be identifiable without undoing the encryption.
ID	KSP-RE-706
Version	1.0
Date	June 18, 2018
Rationale	Law and regulation

Requirement	**Data minimization**
Description	Only strictly necessary information may be collected and only for the purposes for which they are processed.
Supplement	During the development of new services and products must be considered what personal data are needed to provide the service or product to realize data minimization.
ID	KSP-RE-703
Version	1.0
Date	June 18, 2018
Rationale	Law and regulation

Requirement	**Facilitate stakeholder rights**
Description	In the privacy statement must be listed how customers exercise their rights.
Supplement	To be able to provide or erase personal information it must be possible to provide a person concerned with data in a machine readable format (right to data portability or the right to oblivion).
ID	KSP-RE-705
Version	1.0
Date	June 18, 2018
Rationale	Law and regulation

Requirement	**Anonymization**
Description	All (in)directly identifiable information must be removed.
Supplement	Personal data must be processed in such a way, that they are no longer usable to identify a natural person. This means that the processing should be irreversible.
ID	KSP-RE-702
Version	1.0
Date	June 18, 2018
Rationale	Law and regulation