LLINKS Law Offices
通力律师事务所

上海
上海市银城中路 68 号
时代金融中心 19 和 16 楼
邮编：200120
电话：+86 21 3135 8666
传真：+86 21 3135 8600

Shanghai
19F&16F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
Tel: +86 21 3135 8666
Fax: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编：100005
电话：+86 10 8519 2266
传真：+86 10 8519 2929

Beijing
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
Tel: +86 10 8519 2266
Fax: +86 10 8519 2929

香港
香港中环花园道 3 号
中国工商银行大厦 15 楼
电话：+852 2969 5300
传真：+852 2997 3385

Hong Kong
15F, ICBC Tower
3 Garden Road, Central
Hong Kong
Tel: +852 2969 5300
Fax: +852 2997 3385

www.llinkslaw.com
master@llinkslaw.com

Llinks Corporate and M&A Bulletin
January 2018

Twenty Key Points of National Recommendatory Standard for Personal Information Security

By Xun Yang

On 29 December 2017, the Information Security Technique – Personal Information Security Standard (the "*Security Standard*") (which the National Information Security Standardization Technical Commission prepared) has been adopted and is set to be implemented as of 1 May 2018. The Security Standard, to certain degree, clarifies issues in relation to personal information protection and also de facto imposes on business operators higher standards for personal information protection.

The full text of the Security Standard will be publicized on the official website of the National Standardization Commission by the end of this month. This briefing summarizes below twenty key points which are worth noting based on information available.

Effectiveness

1. **Binding Effect**. The Security Standard is not a law per se and has no legally binding effect. However, it would be taken as reference by the government authorities to assess whether business operators have diligently performed their personal information protection obligations under the Cyber Security Law and other laws. For instance, CAC recently requested a meeting with Alipay based on

如果您需要本出版物的中文本，请与下列人员联系：

郭建良: (86 21) 3135 8756
Publication@llinkslaw. com

If you would like other Llinks publications, please contact:

Roy Guo: (86 21) 3135 8756
Publication@llinkslaw. com

Llinks Law Offices
www. llinkslaw. com

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

the ground of, among others, the non-compliance with the spirit of the Security Standard. **As such, the Security Standard should be considered a reference in guiding personal information protection practice.**

Information Security Governance

2. **Responsible Person**. The Security Standard requires that senior management, such as legal representatives and other senior managers, lead information security matters and that, upon satisfaction of certain conditions on the scale of information collection and process, a dedicated division be established to manage information security. The Security Standard provides for the roles and duties of such responsible persons and divisions. **As such, it is not only IT departments' responsibility to maintain information security. Failure to maintain information security may be considered a breach of due care duties of the senior management.**

3. **Security Internal Audits**. The Security Standard requires that business operators carry out information security audit at a frequency of at least once a year to fully review information protection practice, potential risks and security measures. **The internal audits can not only prevent occurrence of actual incidents, but also form a defence when an actual incident occurs.**

4. **Management of Critical Positions**. The Security Standard requires that business operators adopt procedures to ensure that the staff appointed to critical positions, who have access to and process personal information, have good characters, knowledge, and skills, **including to conduct background checks, to deliver trainings and to enter into confidentiality agreements with relevant persons.**

Information Collection

5. **Consent to Indirect Collection**. A direct collection of personal information obviously requires consents by data subjects. In case a business operator collects personal information indirectly from a third party, it must verify the legality of the collection and disclosure of the personal information by such third party. **This requires that business operators not only impose contractual obligations on such third party to ensure the legality of the information disclosure, but conduct necessary due diligence on the source of information as well.**

6. **Exceptions of Collection from Public Sources**. The Security Standard for the first time confirms the legality of collecting personal information from legitimate public sources, such as news reports and government announcements and, thus, **broadens the channels for collecting personal information**.

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

However, the Security Standard fails to clarify the exact scope of legitimate public sources.

7. **Information for Data Subjects**. To seek data subjects' consents to information collection, collectors are required to inform data subjects of their personal information protection policies, including the scope and purpose of the collection as well as security measures to protect the information collected. The Security Standard provides for, in a great detail, the contents and formats of the policies as well as the manners to display such policies. **In particular, business operators need to include enough information in the policies to ensure the sufficiency and, at the same time, to use summaries and highlights to ensure that the policy be clear, reader-friendly and able to attract readers' attentions.**

Storage and Usage

8. **Segregation of Depersonalized Information**. The Security Standard provides for a series of requirements on storage of personal information in possession of business operators. In particular, **if personal identifiers are removed from personal information, physical, technical, and managerial measures must be adopted to segregate the personal identifiers from the depersonalized information to avoid reattaching the personal identifiers back onto the depersonalized information.**

9. **Cessation of Operation**. The Security Standard requires that when business operators cease operating certain products or services, they notify relevant data subjects of the same and delete personal information collected for such products or services. **They must not use such personal information for unauthorized purposes.**

10. **Manner of Usage**. The Security Standard requires that personal information be released as little as possible during the course of usage. In particular, **if end users do not need to know the identifieable personal information, the relevant personal information must be depersonalized before being provided to either internal or external users.**

11. **Deregistration and Withdrawal of Consents**. The Security Standard requires that data subjects be granted the right to deregister their accounts and to withdraw their consents and that data controllers provide channels for such deregistration and withdrawal. **As such, the administrative burdens on business operator which possess personal information are increased.**

12. **Duplicated Copy for Free**. The Security Standard entitles data subjects request for a copy of their personal information in the possession of data controllers and requires that data controllers provide such copies, in principle, free of charge. **This would be an administrative burden for business operators but, based on**

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

reasonable ground and upon proper notification to data subjects, business operators may impose reasonable fees for provisions of such copies.

13. **Opposition of Auto-decision**. The Security Standard requires that if auto-decisions are made based on personal information collected, such as credit ranking, **the relevant business operators provide channels for data subjects to oppose such decision**.

14. **Security Assessment on Sharing Parties**. The Security Standard imposes a number of due care obligations on data controllers which share personal information with third parties, which obligations include **to contractually manage the use of personal information by the parties which receive the relevant personal information and conduct due diligence on their capabilities to protect information security before disclosing any information**.

15. **Disclosure of Sensitive Information**. With respect to the disclosure and sharing of sensitive information, the Security Standard requires that data subjects be informed of such sharing and disclosure as well as the information receivers' security capabilities. **As such, business operators are required to foresee possibilities of future data disclosures and sharing and to be able to balance the clarity and flexibility in describing the parties which are possibly provided with personal information which they collect.**

16. **Information Transfer during M&A**. The Security Standard requires that, during M&As, the parties which take over businesses be responsible for personal information collected for such businesses and for performing the security obligations based on which data subjects give consents for the collections of their personal information. However, the Security Standard fails to clarify whether the transfer of the possessions of personal information during M&As requires data subjects' consents. **As such, data collectors are advisable to consider possible future disposals of businesses at the time of collection, and the parties which take over the businesses are advisable to conduct due diligence on the personal information protection standards applicable to such businesses to be acquired.**

17. **Co-controllers**. Parties, which collect and control personal information jointly (e. g. , e-commerce platforms and the e-shops thereon), are required to document the allocations of their data security duties and responsibilities. **This requires that personal information security and protection clauses be included into relevant commercial agreements (such as Platform Access Agreements).**

Incident Management

18. **Contingency Plan**. The Security Standard requires that data controller prepare contingency plans vis-à-vis

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

possible information security incidents and perform drills accordingly at least once every year. **Such contingency plans and drills can not only prevent occurrence of incidents but also form proofs to certain extent that business operators perform due care obligations in protecting information security.**

19. **Incident Management and Recordal**. The Security Standard requires that business operators manage incidents in accordance with contingency plans and keep proper records of the management. **Such records would be important evidence to determine business operators' responsibilities for the incidents.**

20. **Prompt Notifications to Affected Parties**. During incidents, data controllers are required to promptly notify affected data subjects of the occurrence of the incidents and progresses of resolving the incidents. **This requires that, when preparing the notifications, business operators manage the proper levels of disclosures to avoid insufficient disclosures which cause unnecessary public concerns and reputational damages and also to avoid self-confessions.**

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

Twenty Key Points of National Recommendatory Standard for Personal Information Security

Contact Details

If you would like to know more information about the subjects covered in this publication, please feel free to contact the following people or your usual Llinks contact.

Author	
Xun Yang Tel: (86 21) 3135 8799 xun.yang@llinkslaw.com	

Shanghai	
David Yu Tel: (86 21) 3135 8686 david.yu@llinkslaw.com	**Bernie Liu** Tel: (86 21) 3135 8678 bernie.liu@llinkslaw.com
Selena She Tel: (86 21) 3135 8770 selena.she@llinkslaw.com	**Nicholas Lou** Tel: (86 21) 3135 8783 nicholas.lou@llinkslaw.com
Dali Qian Tel: (86 21) 3135 8676 dali.qian@llinkslaw.com	**Kenneth Kong** Tel: (86 21) 3135 8777 kenneth.kong@llinkslaw.com
David Wu Tel：(86 21) 6043 3711 david.wu@llinkslaw.com	**David Pan** Tel: (86 21) 3135 8701 david.pan@llinkslaw.com
Elyn Jiang Tel：(86 21) 6043 3710 elyn.jiang@llinkslaw.com	
Beijing	
David Yu Tel: (86 10) 8519 2266 david.yu@llinkslaw.com	**Bernie Liu** Tel: (86 10) 8519 2266 bernie.liu@llinkslaw.com
Yuhua Yang Tel: (86 10) 8519 1606 yuhua.yang@llinkslaw.com	
Hong Kong (in Association with Vivien Teu & Co LLP)	
David Yu Tel: (86 21) 3135 8686 david.yu@llinkslaw.com	**Sandra Lu** Tel: (86 21) 3135 8776 sandra.lu@llinkslaw.com

© Llinks Law Offices 2018

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.