Newsletter

Atsumi & Sakai

HANDLING DATA LOSSES :
JAPAN'S NEW REGIME

ATSUMI & SAKAI
TOKYO | LONDON | FRANKFURT
www.aplaw.jp/en

January 2018

SUMMARY

Following the substantial amendments to Japan's Act on Protection of Personal Information ("**APPI**") ("**Amendments**") which came into force on 30 May 2017[1], Japan's Personal Information Protection Commission (the "**Commission**"), the primary data protection authority, has issued general guidelines for handling the loss, etc. of personal information (the "**General Guidelines**")[2]; the General Guidelines set out certain principles for handling such losses, leaving data controllers to decide what specific action they should take having regard to the facts of each case. In this note we outline the requirements and general approach of the General Guidelines, the basic points for data controllers to consider when handling data losses, the Commission's enforcement powers, and the existing practices of data controllers in Japan when handling data losses.

---

1. Actions to be Taken Following a Data Loss

The General Guidelines state that in the event of the leakage, destruction or damage of personal information (together below, a "**data loss**") or the likelihood of a data loss:

(1) it is "desirable" that the affected data controller take the following steps:

a) reporting of the incident within the data controller;
b) taking measures to prevent further damage to the relevant data subjects or third parties actually or potentially affected by the incident (together below, "**affected parties**") due to the incident;
c) investigating relevant facts and the cause of the incident;
d) identifying the affected areas within the servers/systems of the data controller and of the data subjects whose data was affected;
e) "promptly" planning and implementing measures to prevent the recurrence of the incident that may otherwise occur due to the cause of the incident in question;
f) "promptly" notifying the affected data subjects, or making the facts of the breach easily available to them (depending on the facts of each case) for the purpose of preventing the affected data subjects suffering further damage (e.g., to give them the opportunity to take action to avoid or mitigate harm by third parties' use of the lost information); and
g) publicly announcing the relevant facts and the measures to be taken to prevent a recurrence of incident (depending on the facts of each case); and

(2) The data controller must "make efforts" to "promptly" notify the Commission of a data loss unless:

a) the data lost is encrypted "at a high level"[3];
b) all the data lost has been retrieved by the data controller prior to being seen by third parties[4];
c) there is no risk of any specific individual being identified from, or the affected data subjects being harmed by use of, the data lost;
d) the data loss was obviously only internal and not an external leakage; or
e) the leakage is obviously insignificant (e.g., a misdelivery of a parcel where the personal information is only on the delivery address label).

---

[1] A summary of the revisions can be found at ***http://www.aplaw.jp/en/publications/20171221/index.html***. The Amendments include the following changes which may have an impact on foreign companies doing business in Japan and which hold any personal information of individuals in Japan:

(1) Extraterritorial Application of the APPI: Under the Amendments, an offshore data controller which acquires personal information of data subjects in Japan in connection with it supplying goods or services to those persons is now subject to the APPI regime even if it only handles the personal information offshore. If such a data controller suffers a data loss, the Commission may now therefore take regulatory action against it, and although the Commission cannot enforce its orders, etc. against such an offshore data controller, any such order, etc. will be published on the Commission`s website, and the Commission may notify appropriate foreign data regulators of its action.

(2) Abolition of the "5,000" persons exemption: Before the Amendments, a data controller which held the personal information of not more than 5,000 data subjects was exempted from the application of the APPI. The Amendments have abolished this exemption, so any entity holding any personal information of data subjects in Japan is now subject to the APPI regime.

[2] The General Guidelines, in Japanese, are available on the Commission's website at ***https://www.ppc.go.jp/personal/legal/***.

[3] Data is encrypted at a high level when (i) the encryption system is on the list of ISO/IEC 18033 or an appropriate accreditation organisation has confirmed the encryption system as being sufficiently secure, and (ii) the decryption key is remotely controlled or not usable by a third party, or the leaked data or decryption key can be remotely deleted.

[4] This is possible in a case of a loss in paper form or stand-alone hardware, but not for a loss of data to the Internet.

It should be noted that there is no minimum threshold of the number of affected parties below which a report or notification is not required.

2. "Desirable", "promptly" and "efforts"

None of "desirable", "promptly" or "make efforts" is defined or explained in the General Guidelines and their meaning will need to be determined by reference to their common meaning, regulatory and best practice, and the facts of each case, in particular the risk of an innocent party suffering any harm.

It is not uncommon for obligations under Japanese laws and regulations to be expressed as being "desirable" or similar, and in the absence of factors which would dictate otherwise, best practice would be to comply with the obligation unless there is a good reason not to, and the greater the harm non-compliance may cause, the more advisable compliance becomes.

Although "promptly" is not defined, our view is that the nuance of the original Japanese term "*sumiyakani*" would suggest 2 or 3 days in many cases, though this is subject to the facts of each case, in particular whether the affected data subjects may suffer harm and accordingly how urgently they should be notified in order for them to minimise any such harm.

"Make efforts" would be given its normal meaning, though as with "promptly" and "desirable", the greater the actual or potential harm from the data loss, the more advisable compliance with the obligation becomes.

3. Reporting to the Commission

Although a data controller is only required to "make efforts" to notify the Commission of a data loss, best practice would be to submit a report unless any of the exemptions at 1.(2) a) to e) above applies (in which case a report is not required). If the data controller thinks the data loss is not serious enough to warrant a formal report but it is not exempted from reporting, it can seek informal guidance from the Commission on what action to take. If the data loss is very serious, e.g. the loss of bank account details and passwords, the data controller should contact the Commission (and local counsel) at the earliest opportunity, and without waiting to complete the formal report to the Commission. Should a data loss not be reported and the Commission subsequently becomes aware of it, it may require a report be submitted.

The Commission has published a form of data loss report (in Japanese) on its website[5]. The form requires information on the nature and contents of the affected data, the number of affected data subjects, the cause of the incident, whether or not the loss has caused serious harm or is likely to do so (e.g., unauthorised use of lost payment card data), the status of any notification to the affected data subjects and publication of the incident, and measures taken to avoid a recurrence of the loss. After reviewing the report, the Commission may ask questions related to the scale and possible consequences of any harm, damage mitigation or aggravation prevention measures, etc. It may also require follow-up reports to be submitted.

4. Notifying Affected Data Subjects

As mentioned above, affected data subjects should be individually notified of the data loss, or the facts of the loss be made readily available to them; examples of what might constitute making the fact of the loss readily available to the affected data subjects would include placing a sign in an office or other location which they habitually visit, or adding a notice on a webpage directly linked from the home page of the data controller's website.

When considering whether to notify affected data subjects of a data loss directly, or by a more general notice, the two major factors for a data controller to consider are the seriousness of the loss and the harm it may cause, and the effectiveness of the means of notification. If a loss may cause serious harm, the prudent course would be to make it public promptly, and then notify affected data subjects individually (always subject to any directions from the Commission). Where a data controller has decided to give a general notification, it will need to evaluate how effective the means of notification is likely to be; for example, if notification is given on a website, how likely is it that the affected data

[5] ***https://www.ppc.go.jp/files/doc/170530_houkokushoshiki_word.doc***

subjects will visit the website and how long it should be kept active in order to notify an appropriate proportion of affected data subjects. A notification, individual or general, should include a description of the loss and the actions taken by the data controller to mitigate its effects, and it would be advisable to include a phone number or email address which the affected data subjects can use to obtain further information on the loss.

As noted in part 1., depending on the facts of each case, it might be appropriate for the data controller to publicly announce the relevant facts of the data loss, and the measures to be taken to prevent its recurrence; there is no guidance on what form this notice should take, and although it may also be sufficient as notice to the affected data subjects, its effectiveness as such would need to be considered carefully.

Notifications (individual or general) should be given in Japanese, and if any affected data subjects may not understand Japanese, any other appropriate foreign language; they should not be given only in a foreign language unless it is certain that all affected data subjects will understand that language.

5. Investigation and sanctions

If a data loss has occurred and been reported to the Commission, voluntarily or at the request of the Commission, the Commission may investigate the background to the loss, the data controller's data management procedures and the actions the data controller has taken (or not taken) to notify the affected parties (and the Commission). Where the Commission finds defects in the data controller's data management or post-loss actions, it may give guidance to the data controller on what actions to take to improve its data management, or what further steps should be taken to notify affected data subjects of the loss. If the defects are material, the Commission may issue an advice for improvement to the data controller and publish the advice on its website. If the data controller fails to follow an advice for improvement, the Commission may then escalate the matter and issue an order for improvement. (An order for improvement may be issued immediately without a preceding advice for improvement in limited cases of significantly serious data loss.) Failure to comply with an order for improvement would render any individual who is either the data controller or the director or employee of the data controller entity in charge of the system from which the loss has occurred to criminal imprisonment of up to 6 months or a criminal fine of up to JPY 300,000, and the same criminal fine for the data controller if an entity.

If a data controller has not notified the Commission or the affected data subjects of the data loss (or has not publicised the loss if material in either scale or subject matter) and the Commission comes to know of the loss, it might be more likely to find the controller's attitude to compliance unsatisfactory and thus issue and publish an advice for improvement.

Neither the APPI nor the General Guidelines imposes any sanctions for failure to make a report or notification of a data loss, and the General Guidelines only require a data controller to "make efforts" to report a data loss. However, it should be noted that a data controller would be presumed to have breached its duties for data security when it failed to prevent the data loss, and it would probably further be in breach of its obligations if it did nothing following the data loss where action was obviously required. These breaches would justify the Commission issuing an advice for improvement. That said, and as we have noted, it is advisable for data controllers to report a data loss unless a report is not required, and failure to report might be a factor the Commission would take into consideration when deciding whether to issue an advice for improvement. The Commission will publish such advice once issued.

3. Compensation in Practice

To date, data controllers which have suffered a data loss have often voluntarily offered compensation to affected parties, both to forestall any proceedings, and to maintain good public relations; we have not seen any evidence that this practice has been affected by the Amendments. Compensation payments to data subjects (per person) have ranged from JPY500 of e-money, through gift vouchers of JPY10,000, to cash payments of JPY35,000.

If an affected party brings an action against a data controller for a data loss before a court, any judgment by the court would likely be an order against the data controller to pay damages on the grounds of a breach of contract or tort theory. Save for cases such as the unauthorised use of affected

payment card data or the disclosure of sensitive information affecting the personal lives of individuals, the amount of damages an affected party might be entitled to is frequently not large enough to warrant the commencement of proceedings once the costs of the proceedings are taken into consideration.

It should also be noted that it is usually important to treat all affected parties equally. Even if a data controller does not publicise a data breach and only communicates privately with each affected party individually, the widespread use of social media makes the risk of unequal treatment between affected parties being kept private increasingly unlikely, with its attendant negative impact on the data controller's reputation.

Local counsel should be consulted where the data loss affects parties in more than one jurisdiction if the level of compensation differs between the jurisdictions.

4. Sectoral Guidelines and Social Security Numbers

Whilst the General Guidelines only provide that it is "desirable" for an affected data controller to take action, including notifying affected parties and publicising the incident, and that it only has to make "efforts" to notify to the Commission, the Guidelines on Protection of Personal Information in the Financial Area, which have been issued jointly by the Commission and the Financial Services Agency provide that such actions are mandatory in the financial service sector. Similarly, the Commentary on the Guidelines on Protection of Personal Information in the Telecommunication Area issued by the Ministry of Internal Affairs and Communications provide that a breach of secrecy of communications must be reported to the ministry.

"My Number" social security numbers are subject to a separate data protection regime, and any loss of any My Number information must be reported to the Commission[6], though there is no specified deadline for giving the notification. The system for escalation of remedial orders by the Commission is the same as that for losses of other personal information, though failure to comply with an order for improvement could lead to more serious criminal sanctions against both the data controller and any of its officers responsible for the loss than for other data losses. Notification to the affected data subjects is still only "desirable".

Conclusion

Although the General Guidelines represent a welcome step forward in clarifying how an affected data controller should handle a data loss, the general and vague nature of the reporting obligations make it essential that such data controllers consult with local counsel promptly on becoming aware of a data loss.

For further information on these matters, please contact:

Ryuichi Nozaki
Attorney (*Bengoshi*), Japan
Partner, Atsumi & Sakai
E: ryuichi.nozaki@aplaw.jp

Daniel C. Hounslow
Consultant* (UK) to Atsumi & Sakai, Tokyo
E: daniel.hounslow@aplaw.jp

---

[6] The form of report is on the Commission's website at ***https://www.ppc.go.jp/files/doc/271225_gyouseikikann-doppou_houkokuyousiki.doc;*** it is slightly different from the report for other data losses.

Atsumi & Sakai
www.aplaw.jp

Tokyo Office: Fukoku Seimei Bldg.**,** 2-2-2 Uchisaiwaicho, Chiyoda-ku, Tokyo 100-0011, Japan
London Office: 4th Floor, 50 Mark Lane**,** London EC3R 7QR, United Kingdom
Frankfurt Office: Taunusanlage 21 60325 Frankfurt am Main Germany

NOTICES

1. ABOUT ATSUMI & SAKAI

Our firm's name is *Atsumi Sakai Horitsu Jimusho Gaikokuho Kyodo Jigyo*; we are a partnership organized in accordance with the Japanese Civil Code, and we are a foreign law joint enterprise regulated by the Bengoshi Law, the Law on Special Measures concerning the Handling of Legal Services by Foreign Lawyers and regulations of the Nichibenren (Japan Federation of Bar Associations) and bar associations to which our lawyers belong. We are authorised to advise on the laws of Japan, England & Wales, Germany (in association with Janssen Foreign Law Office), the PRC, the States of New York and California, United States federal law, the State of Victoria, Australia and Australian Federal law. For further information, please see our website, www.aplaw.jp.

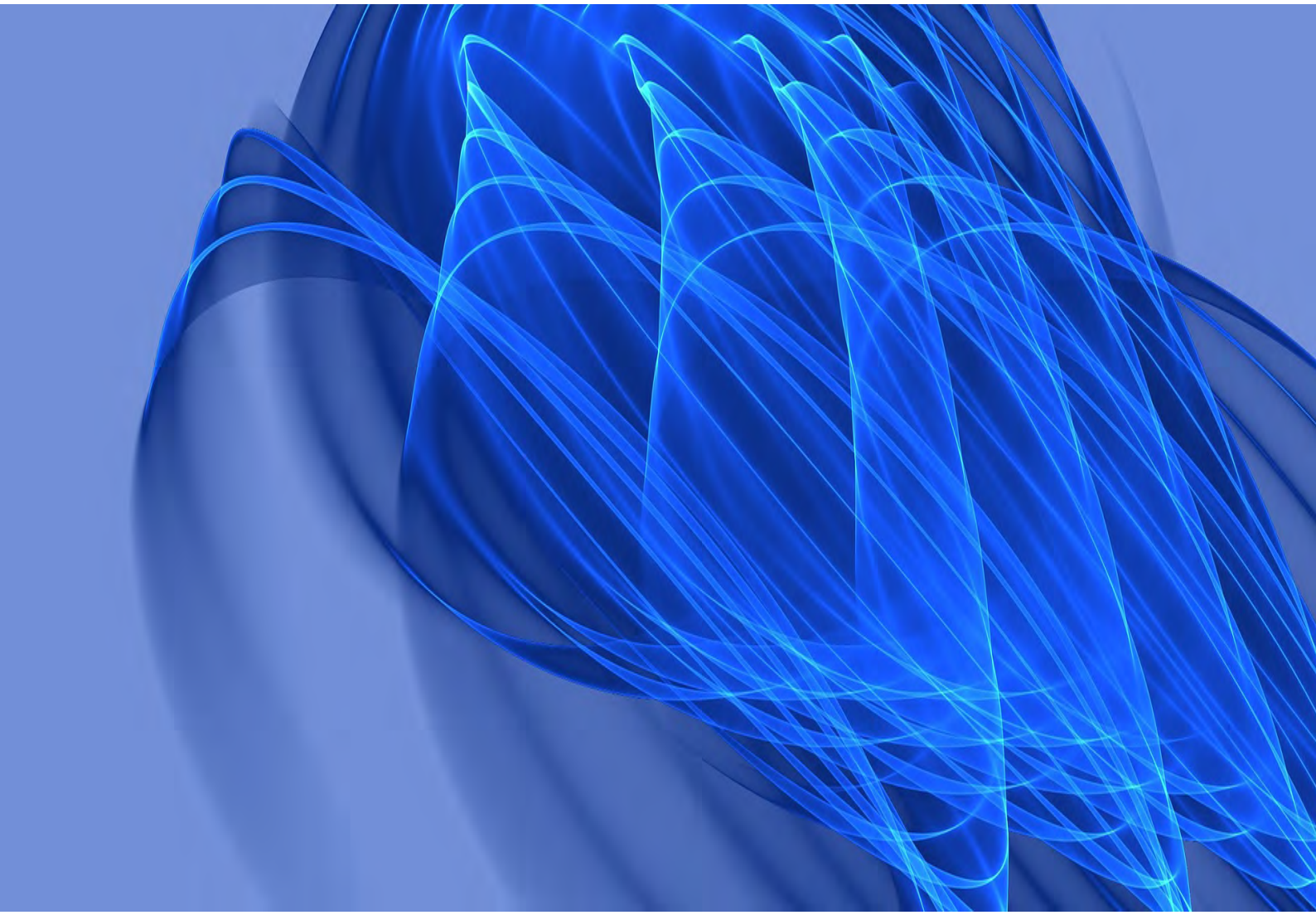
2. JAPANESE LAW ADVICE

Advice on Japanese law will be provided under the supervision and authority of a Bengoshi (Japanese lawyer) Partner or Partners, as identified to you above and/or in correspondence. We will not be liable for any comments or views on Japanese law made by any member of our firm other than a Bengoshi; any such comments or views do not constitute advice on Japanese law and you act on them at your own risk.

3. FOREIGN LAW ADVICE

Advice on any foreign law will be provided under the supervision and authority of a Registered Foreign Lawyer registered to advise on that law in Japan, as identified to you above and/or in correspondence. We will not be liable for any comments or views on a foreign law made by any member of our firm other than a Registered Foreign Lawyer as referred to in this paragraph; any such comments or views do not constitute advice on that foreign law and you act on them at your own risk.

* Mr. Hounslow is a director of Arnaud Advisers Limited (a company incorporated in England and Wales), an independent consultant to Atsumi & Sakai LPC, Tokyo. As such, he is authorised to act for Atsumi & Sakai and in doing so does not act in a personal capacity.



www.aplaw.jp/en/