Key points of the amendment to the Personal Information Protection Act and its impact on the research Industry

Contribution by Japan Marketing Research Association

Here we will discuss four revisions made to the Personal Information Protection Act, presenting their key points and their impact on our industry.

1 Clarification of the definition of personal information

A Personally identifiable data (such as fingerprint data, face recognition data, passport numbers, licence numbers, and mobile phone numbers) added as specific examples of personal information

→ *Criteria for determining whether or not something is considered to be personal information, namely "personal identity" and "easy verification" in conjunction with other information, remain unclear, and discrepancies in interpretation are seen between even companies of our industry. It will therefore probably be necessary to establish such criteria for our industry.*

B Newly establish "information requiring special consideration"

→ *This refers to personal information that requires particularly strict handling (corresponding to "certain sensitive information" defined in JISQ15001:2006). Companies who have been awarded Privacy Mark certification, which is based on this standard, are already in compliance, so the impact on the industry will be minimal.*

2 Ensuring the usability of personal information, etc. under appropriate disciplinary rules

A "Anonymously processed information" is newly established and clearly separated from personal information, ensuring such information's usefulness

→ *Information for which personally identifiable information has been processed (removed) and cannot be restored (made recognisable again) is defined as "anonymously processed information". However, the criteria are unclear with regard to how much processing must be done to make it "anonymously processed information". Criteria established by the Personal Information Protection Commission must be followed, but ultimately it will likely be left up to the independent standards and rules of individual industry organisations.*

→ *Since this does not concern personal information, prior consent from the party concerned is not required, even in cases where it is provided to third parties. However, some measures will be necessary, such as formulating rules on the handling of "anonymously processed information", publicising what items are included in this information, and specifying that the information is "anonymously processed information" when providing it to third parties (e.g. clients). As a result, staff at research firms who handle such information will likely see their workload increase.*

3 Strengthening the protection of personal information

A Mandatory verification and creation of records relating to third-party provision (ensuring traceability)

→ *When providing personal data to a third party (e.g. clients) it has become mandatory to record and save for a certain period of time the date and recipient of the data. In addition, when receiving such information from a third party (e.g. another research firm), it has become mandatory to verify the process by which the provider obtained the relevant personal data, and to record and save for a certain period of time matters relating to the date of provision and verification. In all of these cases, these processes are routinely carried out in this industry in accordance with certain rules, but the point here is that the amended law clarifies the response procedures as far as keeping records.*

B Increased penalties

→ *In our industry (JMRA member companies), most companies have been awarded Privacy Mark certification and are also in a position where they must observe the JMRA Marketing Research Code of conduct. As such, they are unlikely to be subject to the increased penalties, including the newly established "personal information database provision crime".*

C Involvement in provision to third parties without consent of the concerned party (opt-out provision revised)

→ *For industries (JMRA member companies) complying with JISQ15001:2006, which, in principle, does not allow opt-out (prior consent of the concerned party is required for provision to a third party), there will be very little impact.*

D Erasing of personal data added to "ensuring accuracy of data contents"

→ *It is now compulsory for business operators to delete without delay personal data that is no longer needed. However, since the definition of what is "no longer needed" and the scope and method of deleting it are not clear, it will probably also be necessary for our industry to come up with some sort of guideline for handling data that is collected and stored every day from access panels*

4 Coping with the globalisation of handling of personal information

A Limits on the provision of personal data to third parties in other countries

→ *When providing personal data to a third party in another country, if the third party does not meet any of the following requirements, consent for the provision must be obtained from the party concerned: The third party is in a country that meets personal information protection standards equivalent to those in Japan. The third party has a system in place that is compatible with the criteria established by the Personal Information Protection Commission*

→ *When providing personal data to a third party in another country, the exceptional application for third-party provision inside Japan is excluded. Therefore, when entrusting an overseas research company with the handling of personal data, when using an overseas cloud service business, or when using personal data jointly with a group company located overseas, in cases where the other party does not meet any of the requirements above (A), this will be considered to be providing information to a third party, and the consent for the provision must be obtained.*

B Establishment of provisions on the scope of application for handling personal information across national borders

→ *Under current laws, the regulations do not extend to business operators who do not have a base in Japan, but under the amendment, even business operators not based in Japan who obtain personal information in connection with business in Japan will now be subject to Japan's Personal Information Protection Act. This will likely apply to, for example, hosting surveys for overseas research companies (clients) targeting people who live in Japan.*
Due to advances in globalisation and the popularisation of cloud-type services, even in our industry there are more and more cases in providing personal data to a third party in another country or handling personal information across national borders, so the impact of the amendment should not be considered negligible.

Back to table of contents