



Transparency and Accuracy of Personal Data a Win-Win Situation

A guest at a private event asks to view a photograph of him taken by the official event photographer. Does the event organiser accede to his request?

A member of a spa wants to know how her personal data is being used by the company. Does the spa provide her with the information?

Under the Access and Correction Obligation of the Personal Data Protection Act (PDPA), an organisation has to allow an individual access to, and correction of, his personal data that is in the possession or control of the organisation, unless there is an applicable exception.

Meeting these obligations will help the organisation demonstrate transparency and ensure that personal data is updated so that any decision it makes in relation to any individual is based on accurate data about the individual.

As Mr Poh Chee Yong, Data Protection Officer (DPO) of real estate agency ERA Realty Network pointed out, "The data is used for contacting customers, providing updates and for billing purposes, so it is in the commercial interest of both parties to want the particulars to be correct."

In the case of ERA, its clients would have bought or sold a property, or leased or tenanted one, through its salespersons. "Most of the time, if not all, our salespersons would make sure that the personal data is accurate. In the unlikely event that there is an error, it is critical that such information is amended in the first instance," he said.

For ERA, individuals typically call or write in to the DPO – whose email is made available online

together with the company's personal data protection policies – to find out what personal data is in the company's possession or control, and to update or correct it if necessary. To ensure that such requests are promptly addressed, the email address dpo@era.com.sg is checked by both the DPO and the head of the company's IT department, Mr David Seah. Customers can expect a reply within one or two working days, said Mr Poh, who is also ERA's Chief Financial Officer.

Providing Access To Personal Data

Under the PDPA, an access request does not need to be accompanied by a reason. However, asking the requester to be more specific as to what personal data he requires could be helpful to both the individual and the organisation.

For the organisation, it will help them to prepare the information in a way that will be useful to the requester and to do it more efficiently. For example, if an individual is requesting for

"The data is used for contacting customers, providing updates and for billing purposes, so it is in the commercial interest of both parties to want the particulars to be correct."

- Mr Poh Chee Yong
Data Protection Officer (DPO) of
Real Estate Agency ERA Singapore

CCTV footage to ascertain whether he had left a particular piece of belonging in a restaurant at a specific time, providing this information will enable the relevant footage to be prepared more quickly. Alternatively, a written description may suffice in some instances.

For the individual, being more specific with the request will be beneficial as it reduces both the time and costs of access, if applicable. The PDPA allows organisations to levy a reasonable fee based on the incremental costs of providing access, and this fee should fairly reflect the time and effort involved in responding to an access request.

While granting access, organisations should also exercise due diligence and adopt appropriate measures to verify the requester's identity.

Under ERA's personal data protection policy, the company may ask for proof of identity before revealing any information to the requester. Depending on what the company has on record, this proof of identity could take the form of the requester's full name and NRIC, FIN or passport number, or date of birth, residential address, or transaction history if the requester is not comfortable in revealing certain particulars such as his NRIC.

If an organisation receives an access request from an individual, it will have to provide the requester with access to the relevant personal data, as soon as reasonably possible and also information about the ways in which the personal data has been used or disclosed within the preceding 12 months.

This is assuming that the request is not a frivolous one (for example, from a serial requester), and that the burden or expense of providing access would not be unreasonable to the organisation or disproportionate to the individual's interests.

Other exceptions to the Access obligation include cases where personal data, if disclosed, would reveal confidential commercial information that could harm the competitive position of an organisation, or where personal data has been collected, used or disclosed without consent for investigations, proceedings and appeals that have not yet been completed. These are among the exceptions stated in paragraph 1(e) of the Second Schedule and the Third Schedule, and paragraph 1(f) of the Fourth Schedule of the PDPA.

If a request does not fall under any of the exceptions, one question would be how much information does the organisation need to provide? In general, the question of "how" can be answered by indicating the purpose for which the data was used rather than detailing the specific activities involved.

For example, the organisation could indicate that the personal data was used for audit purposes, without going into specific instances on when the audits were carried out. However, when it comes to the ways in which the personal data has been disclosed, it may be more helpful to provide specific names of organisations to

whom the data has been disclosed to. This will allow the individual to approach the third-party organisation for more information should he wish to do so.

One good practice is to maintain a list of all possible third parties that the organisation discloses personal data to, and share this with any individual who puts in an access request.

The information that is given to the individual should be in documentary form, or if it is impractical, the requester should be given the opportunity to examine the personal data and how it had been used or disclosed.

Addressing Errors And Omissions

In addition to acceding to access requests, organisations are also generally required to correct errors or omissions in an individual's personal data upon his request. Under the PDPA, they are not entitled to impose a charge for this.

The correction should be made as soon as it is practical to do so and the amended version sent to every other organisation that the personal data was disclosed to within a year before the date the correction was made; unless that other organisation does not need the corrected personal data for any legal or business purposes. Third-party organisations

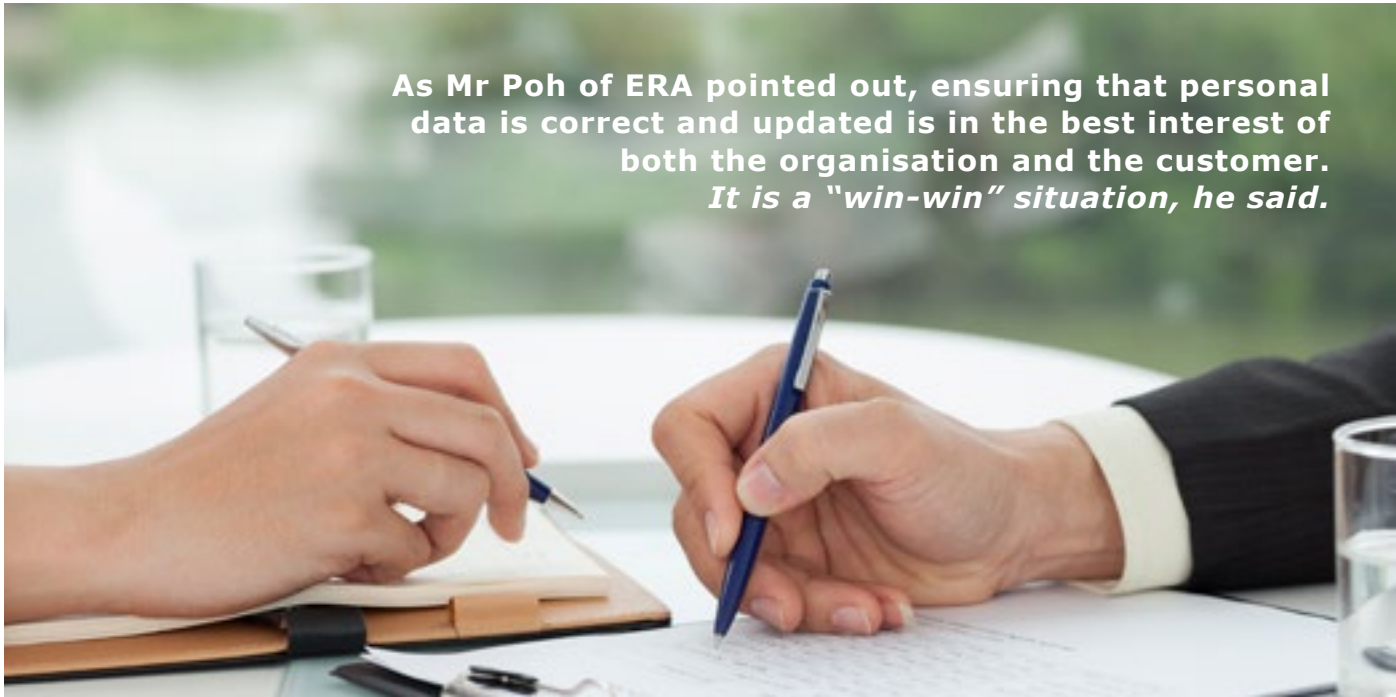
which are notified of the correction will then generally have to correct the personal data that is in their possession. There may, however, be instances where a correction is not made.

For example, a customer may request an online retailer to update his residential address, which forms part of his personal data, and the retailer duly notifies an affiliate that is servicing the customer's warranty. The affiliate may determine that there are reasonable grounds not to correct its records relating to the customer because the customer's warranty has expired. In cases like this, it is good practice to make a note as to why a correction has not been made.

There are also specific circumstances where corrections need not be made, such as those cited in section 22(6) and the 6th Schedule of the PDPA.

Conclusion

It makes business sense to respond promptly and transparently to request for access and correction. A good practice for organisations to adopt would be to institute standard procedures and forms that will help them respond to such requests efficiently and effectively. As Mr Poh of ERA pointed out, ensuring that personal data is correct and updated is in the best interest of both the organisation and the customer. It is a "win-win" situation, he said.



As Mr Poh of ERA pointed out, ensuring that personal data is correct and updated is in the best interest of both the organisation and the customer. It is a "win-win" situation, he said.