Singapore Cricket Association and Another

[2018] SGPDPC 19

Yeong Zee Kin, Deputy Commissioner — Case No DP-1704-B0707

Data Protection – Openness obligation – Requirement to develop and implement policies and practices

Data Protection – Protection obligation – Disclosure of personal data – Insufficient administrative security arrangements

21 August 2018.

Background

1 This case concerns the unauthorised disclosure of the personal data of cricket players on the Singapore Cricket Association's ("**SCA**") websites (the "**Incident**"). On 20 April 2017, the Personal Data Protection Commission (the "**Commission**") received a complaint regarding the unauthorised disclosure of personal data on the player profile pages on the SCA's websites and commenced its investigations thereafter. The Deputy Commissioner's findings and grounds of decision based on the investigations carried out in this matter are set out below.

2 The SCA is the official governing body of the sport of cricket in Singapore. It administers various cricket leagues in Singapore with more than 100 cricket clubs participating across several league divisions. The SCA owns the rights to the domain name www.singaporecricket.org (the "**First Domain**"),

which has served as the SCA's official website since August 2007 ("**Website**"). The SCA also owns the rights to the domain name, www.cricketsingapore.com ("**Second Domain**"). Both domains were accessible to the public and the hosting of both domains were set up and managed by the SCA or on its instructions.

3 All clubs and their players are required to register with the SCA in order to participate in any of the SCA leagues. To register new players, clubs are required to submit the following player personal data through the registration form on the SCA's Website:[1]

(a) Player name;

(b) Player photograph;

(c) NRIC/FIN number;

(d) Date of birth;

(e) Email address; and

(f) Mobile number.

4 Player profile pages which showed the registered player's name, photograph, player code (a unique identifier assigned to players upon registration) as well as player statistics ("**Player Profile Information**") have been made available on the SCA's Website since it was launched in August

[1] Clubs were also required to provide information such as the season, league, division and club the player will be playing in as well as the player's category, role, bowling style and batting style.

(*cont'd on next page*)

2007. Player Profile Information was disclosed on the SCA's Website to identify players participating in the leagues and to promote interest in the sport by providing the public information on the league players in the same way that some soccer and tennis players have public profiles.[2]

5 In February 2016, SCA engaged Massive Infinity Pte Ltd ("**MI**"), a Singapore-based web design and development company, to revamp its Website and design and develop a new custom web portal for SCA ("**Revamped Website**") in accordance with the website development specifications provided to MI.[3] However, as the SCA's website development specifications were set out in very general terms and did not specify the contents of the Revamped Website, details of the exact contents of the Revamped Website were communicated to MI in meetings, and through phone calls and Whatsapp text messages.

6 During the development and testing of the Revamped Website, the Second Domain was used as a trial or user acceptance testing site.[4] In the course of conducting user acceptance tests, the SCA requested the inclusion of some additional pages to the Revamped Website, such as the player profile pages.

---

[2] Given the SCA's long-standing practice of publishing Player Profile Information on its Website, players were deemed to have consented to the disclosure of the Player Profile Information when they registered to participate in the league through their respective clubs.

[3] Together with the Website revamp, the SCA also switched the web hosting company for the First Domain from an India-based web hosting company to one in Singapore. However, MI was only engaged to provide the user interface design and web development of a new custom web portal and did not provide web hosting services.

[4] The Second Domain was removed by the SCA on 17 April 2017 after the First Domain had stabilised. MI had set up a staging environment (scastg.azurewebsites.net domain) ("**Testing Domain**") for development and testing purposes. The Testing Domain was the only web hosting setup maintained by MI for development purposes and was closed soon after the code was pushed to the SCA's testing environment, i.e. the Second Domain, on 17 November 2016. The Testing Domain was not accessible by search engines.

These additional pages were not part of the original design and were therefore not included in the design documents. Neither party was able to produce any evidence of instructions from the SCA on the type of player information that was to be shown on the new player profile pages. While the SCA represented that its intention was for the Revamped Website to show the same Player Profile Information that was on its original Website, it conceded that it did not expressly highlight the type of player information that was to be included on the player profile pages on the Revamped Website.

7 In the absence of any specific instructions on the required fields for the new player profile pages, MI created the new player profile pages based on the information collected from the SCA's player registration page on the Website. Consequently, in addition to the Player Profile Information that had previously been disclosed on the Website, the new player profile pages included fields for personal data such as the player's NRIC/FIN number, date of birth, email address and mobile number (the "**Additional Player Personal Data**").

8 During the investigations, the parties gave conflicting accounts as to when the SCA was first shown the new player profile pages. MI represented that before the new player profile pages with actual player data were pushed to the Second Domain, mock-up player profile pages created using "dummy data" were sent to the SCA for its review. The Revamped Website, including the new player profile pages with actual player data from the database of registered players' data that the SCA had provided to MI ("**Registered Players Database**"),[5] was pushed to the Second Domain for the SCA's review and approval on 17 November 2016. The SCA, however, represented that it had only

[5] The SCA received the database of the registered players' personal data from their previous vendor based in India.

discovered that contrary to its intention, the Additional Player Personal Data was disclosed after MI uploaded the new player profile pages on the Second Domain and subsequently on the First Domain.

9 The SCA and MI held a meeting on 28 November 2016 to review the changes that MI had made to the Revamped Website. However, the SCA claimed that at the time of the meeting, the new player profile pages were missing from the Revamped Website. MI, in turn, stated that as the SCA did not raise any issues with the new player profile pages at the meeting, MI assumed that the SCA had approved the content of the new player profile pages and they were to proceed to production as created.

10 The Additional Player Personal Data was made available on the First Domain on or around 9 January 2017 after the system was migrated from the staging server (i.e. the Second Domain). Upon discovering that the Additional Player Personal Data was disclosed on the new player profile pages, the SCA took steps to remove them from the player profile pages leaving only the Player Profile Information.

11 The Additional Player Personal Data was disclosed on the respective player profile pages and therefore publicly accessible for the following periods:

(a) from the Second Domain, from 17 November 2016 until its removal on 6 February 2017;

(b) from the First Domain, from around 9 January 2017 until its removal on 6 February 2017; and

(c) cached versions of the Revamped Website continued to be listed among the search results on major online search engines until the SCA submitted a request for their removal in May 2017.

12 The parties were unable to determine conclusively the exact number of players whose personal data had been disclosed on the Revamped Website on the First and Second Domains. However, based on the number of pages cached by the search engines, the SCA estimated that as many as 100 players were affected.

Findings and Basis for Determination

13 The main issues for determination are:

(a) whether MI breached section 24 of the PDPA;

(b) whether the SCA complied with its obligations under section 12(a) of the PDPA; and

(c) whether the SCA breached section 24 of the PDPA.

14 It was not disputed that the Player Profile Information and Additional Player Personal Data disclosed on the new player profile pages were "personal data" as defined in section 2(1) of the PDPA.

Whether MI breached section 24 of the PDPA

15 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. MI was engaged by the SCA to

revamp the Website and was subsequently instructed to create new player profile pages on the Revamped Website. The SCA gave MI a copy of the SCA's Registered Players Database in order for MI to upload the players' personal data to the new player profile pages. Accordingly, the Deputy Commissioner is satisfied that the personal data in the Registered Players Database was in MI's possession or under its control at all material times and MI was required to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

16 However, MI intentionally disclosed the Additional Player Personal Data on the new player profile pages because it was under the impression that the SCA had intended for the Additional Player Personal Data to be disclosed on the new player profile pages. In this regard, seeing as MI relied on the SCA for directions as to the personal data that was to be disclosed on the player profile pages and there was no evidence that MI should have known what personal data was to be disclosed from the SCA's instructions or from the circumstances, the Deputy Commissioner finds that MI did not act in breach of its Protection Obligation under section 24 of the PDPA when it disclosed the Additional Player Personal Data.

Whether the SCA complied with section 12(a) of the PDPA

17 Section 12(a) of the PDPA imposes an obligation on organisations to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. The SCA represented, in a witness statement dated 12 June 2017 provided by a representative authorised by SCA, that it did not have any internal guidelines and/or policies for the protection of personal data at the time of the Incident and that it was in the

process of reviewing this and coming up with a data protection policy and guidelines.[6]

18 It bears repeating that the development and implementation of data protection policies is a fundamental and crucial starting point for organisations to meet their obligations under the PDPA.[7] As the Deputy Commissioner highlighted in *Re Aviva Ltd* [2017] SGPDPC 14 (at [32]) on the role of general data protection policies:

> Data protection policies and practices developed and implemented by an organisation in accordance with its obligations under section 12 of the PDPA are generally meant to increase awareness and ensure accountability of the organisation's obligations under the PDPA.

19 In this regard, the Deputy Commissioner agrees with the observations in the Joint Guidance Note issued by the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia that employees will be able to better protect personal data when they are able to first recognise when a matter involves data protection:[8]

> Training and general education on privacy are very important. Our Offices have seen instances where issues were not identified as privacy issues when they should have been. As a result, appropriate steps were not taken to prevent or address privacy breaches. In other cases, we have seen a lack of

---

[6] The SCA had a data protection officer but its data protection officer had not undergone any training on data protection matters.

[7] *Re M Star Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15 (at [25]).

[8] Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia, Getting Accountability Right with a Privacy Management Program <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/> at p 13.

> awareness or appreciation for privacy risks on the part of employees result in the development of products or services that were not compliant with applicable privacy law. In Alberta, human error is the most common cause of reported breaches resulting in a real risk of significant harm to an individual. Examples include: misdirected faxes and mail, e-mail addresses viewable in mass e-mails, inappropriate disposal of documents, and disclosure of passwords.
>
> Employees will be able to better protect privacy when they are able to recognize a matter as one that involves personal information protection.
>
> [Emphasis added.]

20 Therefore, by the SCA's own admission, it failed to meet its obligations under section 12(a) of the PDPA.

Whether the SCA complied with section 24 of the PDPA

21 The SCA obtained the Registered Players Database, which contained the personal data of all its registered players, from its previous vendor based in India. A copy of the Registered Players Database was handed over to MI "for a week" for MI to upload the players' data onto the new player profile pages. The SCA alone had the right to determine whether and how many of the players' personal data would be held and presented in the Revamped Website. Hence, the Deputy Commissioner is satisfied that the personal data in the Registered Players Database remained under the SCA's control at all material times.

22 Having considered the matter, the Deputy Commissioner finds that the SCA failed to put in place reasonable security arrangements to protect the personal data in its control and therefore acted in breach of its Protection Obligation under section 24 of the PDPA.

23 Player profile pages were in the SCA's original Website and the SCA's eventual actions disclose its intention to retain player profile pages as a function

of the Revamped Website. As stated in paragraph **Error! Reference source not found.** above, the SCA did not provide sufficiently detailed requirements to MI. The omission of the player profile pages was eventually discovered during user acceptance testing. The SCA then requested that player profile pages be retained in the Revamped Website. Again, the SCA did not provide detailed requirements specifications and MI was left to devise player profile pages based on the information provided by players via the online registration form. Needless to say, this disclosed too much personal data.

24 Despite the fact that the inclusion of player profile pages had been made during the final stages of the project, the SCA failed to follow up to check that this function of the Revamped Website had been properly implemented. Such an omission is particularly egregious given its context and chronology. A flaw in the Revamped Website had been identified by the SCA and certain directions had been given to MI. One would expect that the natural behaviour of the owner of a website would be to ensure that identified flaws are properly fixed. The omission of the player profile pages and how this has been resolved by MI ought to have been in the SCA's consciousness. This betrays the SCA's lackadaisical attitude towards protection of the personal data of registered players and sets the context for the severity of its negligence which is examined below.

25 First, the SCA provided a database of all existing players in its Registered Players Database to MI. It should have clarified whether its intention was for all the personal data in the Registered Players Database to be displayed in the new player profile pages. The SCA simply assumed that MI would replicate the same fields in the previous player profile pages. As owner of the Revamped Website, the onus is on the SCA to give clear instructions to MI. As a result of the SCA's failure to state in clear terms the required fields to be created in the new player profile pages, the Additional Player Personal Data of

as many as 100 registered players were disclosed on the First and Second Domains.

26 Second, considering that the registered players' personal data would be disclosed in the new player profile pages, the SCA ought, at the very least, to have reviewed the new player profile pages before MI uploaded it to the First and Second Domains. Had the SCA done so, the disclosure of the Additional Player Personal Data could have been avoided. It bears repeating that this omission is especially egregious given the fact that the SCA had identified a flaw, which would have meant that this omission should have been in its consciousness, but it failed to follow up with ensuring that it had been properly addressed.

27 Simply assuming that MI would replicate the same fields in the previous player profile pages is a clear derogation of its protection obligation. The provision of proper and clear instructions to the designer and developer of a website that holds personal data can and should form part of the protection obligations of the organisation that owns it. In failing to do so, the SCA is in breach of the protection obligation. Further, as mentioned above, the Deputy Commissioner found that the SCA's website development specifications lacked website content details. As a result, instructions and details of the SCA's requirements were conveyed to MI piecemeal in meetings and through phone calls and Whatsapp text messages, which appears to have led to confusion and miscommunication between the parties as to the exact requirements for the Revamped Website.

28 Regardless of whether the SCA was shown the new player profile pages at the 28 November 2016 meeting or earlier, the Deputy Commissioner finds

that at least between 28 November 2016 and 6 February 2017,[9] the SCA could have and ought to have, but failed to, discover and prevent the unauthorised disclosure of the Additional Player Personal Data on the new player profile pages. However, the SCA was unable to explain why it had failed to pick up on the unintended disclosure of the Additional Player Personal Data earlier or provide sufficient information on what arrangements or measures (if any) were implemented to review the changes made to the Website.

29 At this juncture, the Deputy Commissioner reiterates that organisations that engage service providers to process personal data on their behalf should clarify and properly document the nature and extent of service provided.

30 This was highlighted in *Re Smiling Orchid (S) Pte Ltd and Ors.* [2016] SGPDPC 19 (at [51]) where the Commissioner emphasised the need for a clear meeting of minds as to the services the service provider has agreed to undertake:

> It is unclear whether T2's actions would have been different had it been engaged to do more than enhancing the design of the site. Data controllers that engaged outsourced service providers have to be clear about the nature and extent of services that the service provider is to provide. There must be a clear meeting of minds as to the services that the service provider has agreed to undertake, and this should be properly documented. Data controllers should follow through with the procedures to check that the outsourced provider is indeed delivering the services. In the absence of such clarity of intent and procedures, it is risky to hold that the outsourced service provider is a data intermediary. In any case, the Commission has found that T2 is not a data intermediary for the reasons set out at paragraphs 35 to 38 above.

[Emphasis added.]

---

9 As mentioned above, the SCA removed the Additional Player Personal Data from the First and Second Domains on 6 February 2017.

31 Also, as highlighted in the Guide on Building Websites for SMEs (at [4.2.1]), organisations that engage IT vendors to develop and/or maintain their websites should ensure that their IT vendors are aware of the need for personal data protection:

> Organisations should emphasise the need for personal data protection to their IT vendors, by making it part of their contractual terms. The contract should also state clearly the responsibilities of the IT vendor with respect to the PDPA. When discussing the scope of the outsourced work, organisations should consider whether the IT vendor's scope of work will include any of the following:
>
> - Requiring that IT vendors consider how the personal data should be handled as part of the design and layout of the website.
>
> - Planning and developing the website in a way that ensures that it does not contain any web application vulnerabilities that could expose the personal data of individuals collected, stored or accessed via the website through the internet.
>
> - Requiring that IT vendors who provide hosting for the website should ensure that the servers and networks are securely configured and adequately protected against unauthorised access.
>
> - When engaging IT vendors to provide maintenance and/or administrative support for the website, requiring that any changes they make to the website do not contain vulnerabilities that could expose the personal data. Additionally, discussing whether they have technical and/or non-technical processes in place to prevent the personal data from being exposed accidentally or otherwise.
>
> [Emphasis added.]

32 Therefore, in light of the above, the Deputy Commissioner finds that the Organisation failed to make reasonable security arrangements to prevent unauthorised disclosure of the Additional Player Personal Data and is therefore in breach of section 24 of the PDPA.

Directions

33 Having found that the SCA is in breach of sections 12(a) and 24 of the PDPA, the Deputy Commissioner is empowered under section 29 of the PDPA to give the SCA such directions as it deems fit to ensure compliance with the PDPA.

34 The Deputy Commissioner took into account the following factors in assessing the breach and determining the directions to be imposed:

Aggravating factors

(a) the personal data disclosed included the registered players' NRIC/FIN numbers;

Mitigating factors

(b) the SCA took prompt action to mitigate the impact of the breach by removing the Additional Player Personal Data from the player profile pages on the First and Second Domains soon after it discovered the Incident; and

(c) the SCA cooperated fully in the investigation.

35 Having considered all the relevant factors of this case, the Deputy Commissioner hereby directs the SCA:

(a) to develop and implement policies and practices that are necessary for the SCA to meet its obligations under the PDPA within 90 days from the date of this direction;

(b) to conduct personal data protection training for its employees to ensure that they are aware of, and will comply with the requirements of the PDPA when handling personal data within 90 days from the date of this direction; and

(c) to inform the office of the Commissioner of the completion of the above directions within 7 days of implementation.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION
