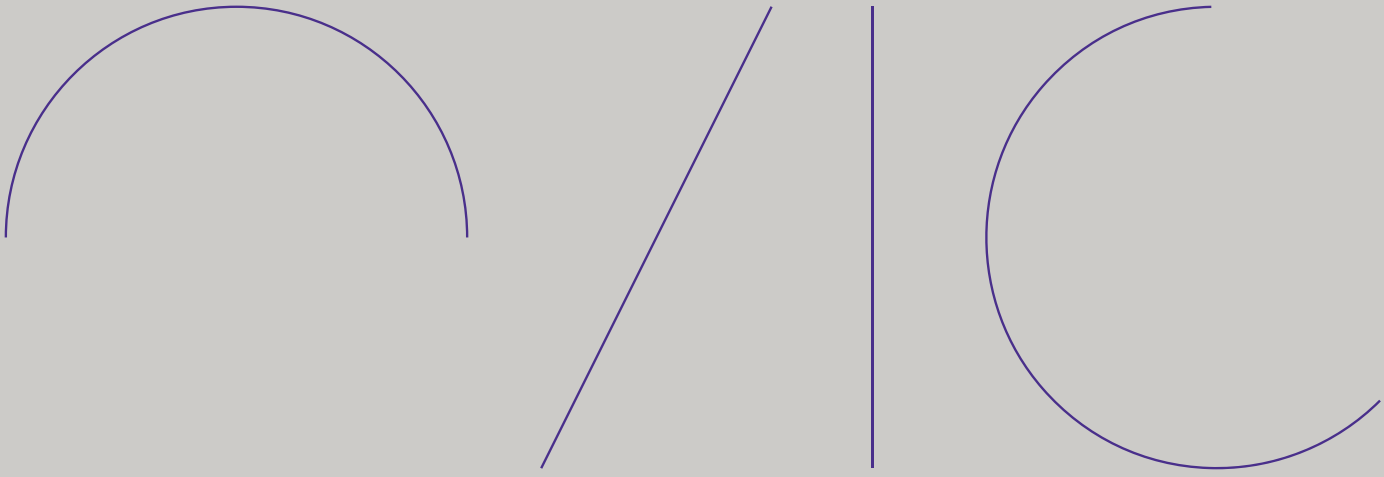
OVIC
Office of the Victorian Information Commissioner

Report on the privacy impacts of Greater Western Water's migration to a new billing and payment system



August 2025

Disclaimer

The information in this document is general in nature and does not constitute legal advice.

Copyright

Table of Contents

Background

1. Greater Western Water (**GWW**) is a Victorian Government water corporation which was formed in 2021 by a merger between City West Water and Western Water. It provides water and recycled water supply, sewerage and trade waste services to approximately 568,000 residential customers and over 47,000 business customers across Melbourne and the western region.

2. On 29 May 2024, GWW launched a new billing and payment system named *CustomerPlace*. This was designed to replace the billing systems from its two precursor organisations. GWW noted that the two previous systems – Aquarate and Gentrack – were old and did not offer features that customers expect from a water company.

3. From the outset, the new system was troubled by a range of technical issues. While this report focuses on privacy impacts caused by the move to *CustomerPlace*, there were other problems for GWW and its customers – such as delayed bills[1] or incorrect billing amounts.

4. The main privacy concerns relate to personal information being disclosed to unauthorised third parties by the new system – due to issues such as bills being delivered to the wrong address, or addressed to the wrong person.

5. The Office of the Victorian Information Commissioner (OVIC) conducted preliminary inquiries into GWW's move to *CustomerPlace* to gather information about the cause and extent of the privacy impacts on its customers, and to consider whether to launch a formal investigation under section 8C(2)(e) of the *Privacy and Data Protection Act 2014* (**PDP Act**).

6. OVIC undertakes such investigations to determine whether there have been serious, flagrant or repeated contraventions of the Information Privacy Principles (**IPPs**), and whether to issue a compliance notice. A compliance notice requires an organisation to take specified action within a specified timeframe to ensure that it complies with the IPPs.

7. Although Deputy Commissioner found the data breaches to be both serious and repeated, she decided not to launch a full investigation into GWW because:

    - The nature and complexity of the underlying causes of the privacy impacts – in terms of inaccurate personal information resulting from a defective data integration process – were such that it was unlikely that OVIC would be able to define specific actions as part of a compliance notice to ensure that GWW could remedy the situation and ensure compliance with the IPPs.

    - The likely time and resources it would take for OVIC to carry out an investigation were not commensurate with the potential benefits of doing so. GWW continues to actively attempt to

[1] Essential Services Commission [website], (29 September 2024), 'Greater Western Water: delayed billing', https://www.esc.vic.gov.au/media-centre/greater-western-water-delayed-billing, accessed 17 April 2025.

remedy issues related to inaccurate personal information in its new system and is incentivised to do so.

8. The Deputy Commissioner nevertheless considered there was a public interest in publishing a brief report on this matter under section 111(3) of the PDP Act.

9. This is because the preliminary inquiries identified significant shortcomings in GWW's preparations for moving to its new billing and payment system, which have had significant privacy impacts for its customers. Therefore, a high-level overview of OVIC's findings is likely to provide valuable lessons for other agencies when undertaking data migration or integration activities as part of system upgrades or other significant operational changes.

Privacy impacts of the migration to a new system

10. Shortly after *CustomerPlace* went live on 29 May 2024, GWW began receiving reports from customers about incidents of personal information being sent to unauthorised third parties (**privacy incidents**). By June 2025, GWW had reported to OVIC that there had been 320 such privacy incidents associated with *CustomerPlace*.

11. These privacy incidents have included issues such as:

    - Bills being sent to the wrong individual, for example, estranged family members or ex-partners, current or previous tenants, previous owners, customers with similar names, residential customers receiving bills for a business address, or simply, other unrelated individuals.

    - Bills being sent to the wrong physical address or email address, which can include previous address, residential versus investment address, seasonal address, or other unrelated addresses.

12. Where a bill is sent to an unauthorised third party, this may reveal information such as names and addresses, as well as account information, billing details, and property holdings. This carries a risk of harm to affected customers, particularly where a new address is revealed to a known-individual to whom they did not wish to reveal such information – such as a perpetrator of family violence or estranged family member.

13. GWW has become aware of the 320 privacy incidents mainly through the unintended recipients reporting that they have received someone else's bill in error. However, in OVIC's view it is likely that the true number of privacy incidents is significantly higher, given that:

    - Privacy incidents are ultimately caused by the fact that some information on *CustomerPlace* is inaccurate – and that despite its efforts GWW cannot easily identify all information that is inaccurate in its system and fix this.

- It is reasonable to assume that not all unintended recipients of bills sent to them in error will take the time and effort to contact GWW to report this, particularly if they do not wish to draw attention to the fact they have obtained personal information they should not have.

14. Despite this lack of visibility about the extent of privacy incidents, it was not until March 2025, following receipt of guidance from OVIC, that GWW published communications on its website informing customers about the privacy impacts of its migration to *CustomerPlace*.

15. These communications set out that it was possible that customers had been, and continued to be, affected by inaccurate information in the new system, without GWW being aware of it. It also informed customers of steps they could take to ensure their information was accurate by logging into their online account and verifying their details, so they would not be subject to a privacy incident. It is the Deputy Commissioner's view that GWW should have taken this step much sooner.

16. As well as impacting its customers, the flawed implementation of *CustomerPlace* has had significant impacts on GWW. Considerable time, funding, and human resources have been required in its attempts to fix the problems caused by inaccurate information in its new system. Its reputation has been negatively impacted, it has suffered financial loss, and it has been subject to investigations or inquiries by multiple regulatory bodies and an independent review.

Causes of the privacy impacts

17. As noted, one of the principal causes of the privacy impacts on customers has been deficiencies in the accuracy of information on *CustomerPlace*. This happened in part because of the way in which GWW and/or its contractors managed the migration of information from two legacy billing and payment systems to the new one while also making changes to other so-called "satellite" systems that also provided data.

18. The process of data migration appears to the uninitiated to be a simple one. GWW sought to move all customer details from two legacy systems and insert these into the new system. However, there are several ways in which to manage data migration, and different methods carry different risks. Assessing the risks and having appropriate controls in place requires experience and good governance. Migrating two systems at the same time into a new structure, which necessitates the process of data integration, magnifies the risk considerably. Doing this while also implementing changes to source systems – such as those that managed data related to customer premises – made the project even more complicated.

19. Broadly, GWW's data integration project was flawed in terms of the quality of the data, weaknesses in test processes, and the data governance arrangements, including risk assessment processes.

Data quality

20. The most essential component of an effective data integration process is data quality – understanding the content of the existing databases, the structure of the databases, and any format or rules constraints in the existing data that may require cleaning or modification in order to work correctly in the new database.

21. After cleaning up missing information in the existing data, care must be taken to ensure that any inconsistencies in the format of existing data map cleanly to the format in the new database: for a hypothetical example, that all dates are expressed in the same way (e.g. DD-MM-YYYY vs DD-MM-YY, or MM-DD-YYYY as Americans express it). Even small details, such as whether names can contain apostrophes, or how many characters are allowed in any field, are crucial. This may mean that very different data harmonisation tasks are required for each source data set. A major difference in source data – for example whether an address is a postal address or a residential address, or billing address, will cause an error in mapping to the new database.

22. During this process, changes to other source systems (anything that feeds data into the old system, or the new system) should be minimised. Any changes that are made to such systems should require end-to-end testing of all systems together.

23. As mentioned earlier, the challenges of integrating two data sets into a new system magnify the risk in the project. In a data migration project involving a single source, after data has been migrated from one source database to the new one, reconciliation is undertaken to ensure that all the data has been transferred and is accessible. In an integration project, once the second database has been ingested this gets harder, because the new database with both sources in it now does not map directly back to either source system but is (theoretically) a composite of the two. Data validation is therefore especially crucial, through a series of tests that can be applied to the new data store. Depending on the complexity of the datasets, these tests are often extensive and can consume significant time and resources.

24. Typically, all these processes to this point are undertaken in a test environment using staging servers, so that testing can be undertaken and additional quality assurance processes applied before moving harmonised data to the production server/s.

25. During the development of *CustomerPlace*, GWW itself was building the system that managed data relating to customer premises. Because this was treated as a separate project, GWW's vendor/s for the *CustomerPlace* project were unable to do end-to-end testing including the full range of data from all systems.

26. An essential control in the cutover from a legacy system to a new one is to have a "rollback" or failover mechanism in which – if the new system demonstrates any unforeseen issues – the legacy system/s can be restored and continue to operate until the issues are resolved and the cutover can be attempted again.

27. In a live billing system such as *CustomerPlace*, a rollback becomes considerably more difficult with the passing of time, as there will be new information in the new database that does not exist in the legacy system, and a rollback could have the effect of losing this information.

28. Another factor that complicated GWW's ability to rollback to previous source systems was that – concurrent with go live – the tariff for billing was due to change due to regulation. Ideally, work on the *CustomerPlace* system should have paused to allow for the implementation of the new tariff in the existing systems, and for testing based on those to be undertaken before go live was considered. However Aquarate and Gentrack were not modified to account for the new tariff, on the assumption that they would not be in use after cutover to the new system (the decision may have been influenced by the age of the infrastructure Gentrack was operating on, which was out of its support contract, and the cost of undertaking the work).

29. This decision – to implement the tariff changes on the new system, but not on the legacy systems – meant that rollback to those systems could not have been undertaken without loss of revenue.[2]

30. At the outset, GWW was aware that there were issues with the quality of data in the two legacy systems which, if unaddressed, would have caused defects when inserted into *CustomerPlace* (which has different data structures and data validation rules). GWW described some of these issues as follows:

    The source data in the two legacy systems included inactive and dummy accounts, out-of-date customer contact details, and manual workarounds; issues that were compounded by the complexity of the data structure conversion from the legacy systems to CustomerPlace. Examples of the data structure not conforming include the legacy systems allowing four customer address methods compared with CustomerPlace only allowing three; inconsistent or inaccurate formatting of phone numbers; and different traceability methods for customers between the legacy and new systems.

31. GWW therefore established a dedicated data cleansing taskforce comprising 23 full-time equivalent positions in November 2023. Data cleaning was conducted primarily by GWW.

Data validation

32. As part of its data cleansing process, GWW and/or its contract service providers came up with 81 data validation rules. These rules required that various data elements must meet defined criteria to ensure they comply with quality and integrity requirements to work properly in the new system. The data validation process is a way of checking that all the mandatory fields in the new system are populated with compatible data, and that unnecessary or inaccurate data are excluded.

[2] This summary of the problems with rollback is simplified and does not consider cost issues, and the Deputy Commissioner acknowledges that these are always considerations in any project, but regardless of whether or not it was cost effective, the lack of a rollback option represented a critical risk. In hindsight, the cost of carrying out work on the legacy systems may have been less than the very high costs associated with the failure of the project.

33. GWW's data validation rules covered factors such as data values and formats, and the relationships between different fields. However, a rule to validate a customer's preferred billing method (e.g. e-billing versus postal address, Bpay vs postal address) was not included in the validation set. The result was that any account listed with a preference of "e-bill or Bpay" in a legacy system defaulted to postal address in the new system when it was migrated.

34. Of greater significance, it appears that as the date that had been set for *CustomerPlace* to go live (end May 2024) approached, either GWW or its vendors decided to reduce the robustness of this validation process.

35. That is, some of the validation rules were removed, so that accounts that would not otherwise have met the set criteria could be loaded into the new system in time for the go live date. Some tables in the database data were not reconciled with other related tables.

36. This information on removal of validation rules was provided by GWW. A vendor engaged for the integration work explained that the rules were related to filters applied to data before its inclusion in the new *CustomerPlace* data set, and that the removal of these filters resulted in 99 per cent of all existing records being included in *CustomerPlace*.

37. The vendor suggested that this improved the robustness of the data set. The Deputy Commissioner was unable to reconcile this suggestion with the issues surrounding data quality problems encountered after go live and, consistent with the problem of being unable to test end-to-end, observed that it would be unclear where data integrity issues arose. At the time of go live it appears that one or all of the parties involved did not have a clear picture of outstanding data quality issues.

38. This decision came at the cost of data quality. It meant there were many accounts migrated into the new system that did not meet original data validation rules. Regardless of which parties involved in the project made the decision, it was ill-considered.

39. The vendor said that agreed treatment plans were in place for all issues that had been identified up to that point. Obviously, in light of events subsequent to go live, there were issues that had not yet been identified.

40. There was an assumption by the vendor/s and GWW that any inconsistencies could be fixed manually after the system went live.

41. GWW and the vendor documented the changes in GWW's Jira ticketing system, but the impacts of these changes were not fully appreciated by the GWW project board.

42. The GWW executive was only made aware of the changes made to the data validation process during the final test of the new system in May 2024. Despite this, the executive made the decision to go live on 29 May 2024, based on the projected data success indicators and treatment options recommended by vendor/s.

43. The Deputy Commissioner considered that the failure of effective communication of risks between the vendor and the client led to the project board having an inadequate understanding of the risks of going live with the system. While commercial imperatives were likely driving the desire to meet timelines, if

GWW had fully understood the scope of the potential errors and the costs of remediation it is doubtful that the project board would have given approval for going live.

44. The result of this imperfect understanding was the exposure of many customers' details to incorrect recipients.

45. GWW has noted that, in hindsight, it realises that rather than reducing the validation steps, additional validation steps should have been implemented. For example, validation to ensure that only the active customer address was migrated to the new system from the legacy systems.

46. Since *CustomerPlace* went live, GWW has noted that it has manually updated 320,000 records where it has proactively identified inaccuracies, or where customers have reported inaccuracies (inaccuracies have related to customer, property and meter related issues).

47. Despite the considerable efforts made by GWW to rectify the situation, the fact that there are ongoing reports of privacy incidents indicates that there continues to be inaccurate information in the *CustomerPlace* system.

Lessons

48. While a detailed analysis of the technical aspects of the *CustomerPlace* data migration process is beyond the scope of this report, and no conclusions should be drawn as to whether GWW or its vendors were primarily at fault, it stands as a case study from which lessons can be drawn by other organisations undertaking similar data migration projects.

49. Most strikingly, this case demonstrates that data migration (and – in particular – data integration) is usually a complex and intricate undertaking. Where there are flaws in the planning and execution of migrating data to a new system, the privacy impacts can be significant, widespread, and difficult to remediate.

Planning

50. Data migration projects should be carefully planned. Data integration projects require special care. This involves dedicating sufficient time and resources to achieve accurate and high-quality data in the new system.

51. Changes to source systems should be minimised. Conducting parallel development projects where one system is dependent upon another increases overall project complexity and risk. End-to-end testing of the entire data ecosystem must be undertaken.

52. The planning phase of a data migration project should include an assessment of the expertise required for the particular project, so that team members with the relevant skills, knowledge, and experience can be assigned.

53. It is not just operational team members who need to have sufficient knowledge of the nature of the project and its risks. It is crucial that the body providing oversight of the project – usually the executive, the board, and preferably both – are fully informed about these matters. This must involve a clear understanding of the potential privacy impacts that could arise if the implementation of the data migration project is flawed.

54. Planning should include clear contingency arrangements that can be implemented if aspects of the data migration do not go to plan. That may mean, for example, an organisation can roll back to using its old systems if it transpires that its new system is not functioning properly with the migrated data. However, the window for doing this in a production system is very tight – any rollback involves lost data for the period between go live and the rollback, and where the system involves billing this can present cost issues in terms of foregone revenue.

Implementation and oversight

55. There are inherent difficulties in moving data from legacy systems to a new system that has different structures and different rules. The sheer volume of data can also pose challenges that should be carefully managed. As a result, the implementation of a data integration project should be conducted in a careful and staged way.

56. While commercial considerations may preclude this, it may be more prudent to consider the migration and integration steps as discrete projects, that is, migrate one legacy system to the new data platform, ensure it is working properly, and then integrate the data from the second source system.

57. Alternatively, another mitigation step might be to delay go live until a full set of end-to-end tests pass. This would also have cost implications (especially since, in this case, tariff changes needed to be implemented in source systems), but may be more cost effective than the post-go-live iterative fixes the vendor and GWW have been engaged in for over a year since the decision to go live was taken.

58. At the outset, the project team should come up with a more comprehensive data migration strategy. This should involve, for example:

    - Carefully mapping out the data structure of the new system and formulating data validation rules (i.e. only data that complies with the rules will be loaded into the new system).
    - Reviewing the legacy system/s to determine what types of data will be necessary in the new system.
    - Pausing any prospective changes to source systems. If this is not possible, the integration project should be delayed until those changes have been made, and tested thoroughly.

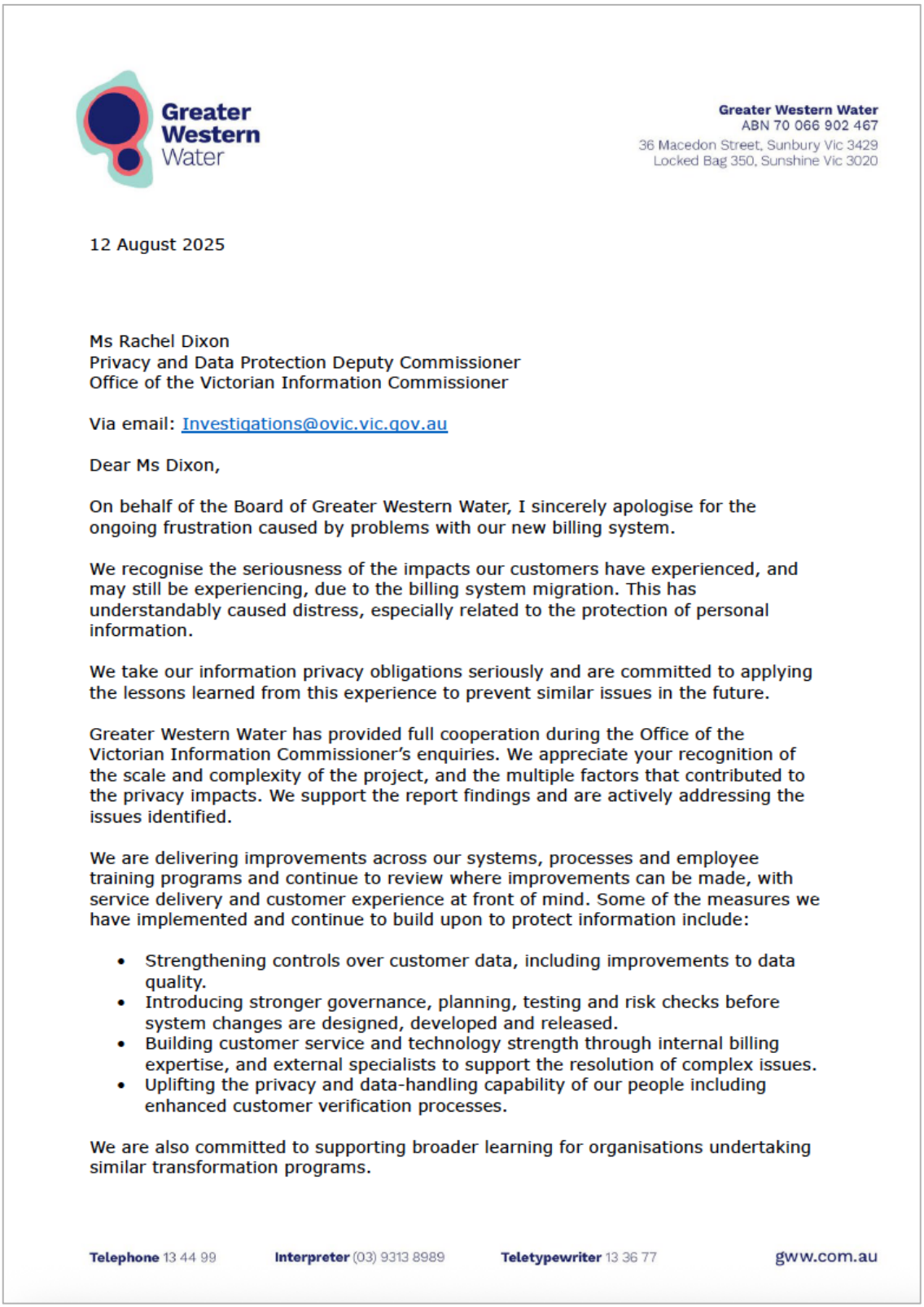
- Performing an initial cleanse of this data in the legacy system/s (such as by deleting duplicate or dummy accounts).
- Assessing data in the legacy system against data validation rules, and making any required changes to ensure compliance with these rules.
- Unit and system tests throughout the migration/integration process, including end-to-end tests.
- Migrating all data into the new system and conducting rigorous testing to ensure that all aspects of the new system are functioning properly.

59. "What if" scenario planning should be conducted before taking any system into production. Rollback, while generally inconvenient and costly, should be available as a contingency plan.

60. There must be clearly defined roles and responsibilities throughout the project. In particular, from the board and executive level down to the integration team (and any others in between) it should be clear where authority lies for making different decisions – such as deciding to make changes to the data migration strategy or data validation rules.

61. Organisations should not prioritise deadlines and timing at the cost of individuals' privacy. While it may be frustrating to miss intended dates for a system to go live, the GWW experience demonstrates that reducing the robustness of a data validation process may have more negative impacts than a project delay.

Annexure A



Greater Western Water

Greater Western Water
ABN 70 066 902 467
36 Macedon Street, Sunbury Vic 3429
Locked Bag 350, Sunshine Vic 3020

12 August 2025

Ms Rachel Dixon
Privacy and Data Protection Deputy Commissioner
Office of the Victorian Information Commissioner

Via email: Investigations@ovic.vic.gov.au

Dear Ms Dixon,

On behalf of the Board of Greater Western Water, I sincerely apologise for the ongoing frustration caused by problems with our new billing system.

We recognise the seriousness of the impacts our customers have experienced, and may still be experiencing, due to the billing system migration. This has understandably caused distress, especially related to the protection of personal information.

We take our information privacy obligations seriously and are committed to applying the lessons learned from this experience to prevent similar issues in the future.

Greater Western Water has provided full cooperation during the Office of the Victorian Information Commissioner's enquiries. We appreciate your recognition of the scale and complexity of the project, and the multiple factors that contributed to the privacy impacts. We support the report findings and are actively addressing the issues identified.

We are delivering improvements across our systems, processes and employee training programs and continue to review where improvements can be made, with service delivery and customer experience at front of mind. Some of the measures we have implemented and continue to build upon to protect information include:

- Strengthening controls over customer data, including improvements to data quality.
- Introducing stronger governance, planning, testing and risk checks before system changes are designed, developed and released.
- Building customer service and technology strength through internal billing expertise, and external specialists to support the resolution of complex issues.
- Uplifting the privacy and data-handling capability of our people including enhanced customer verification processes.

We are also committed to supporting broader learning for organisations undertaking similar transformation programs.

Telephone 13 44 99 **Interpreter** (03) 9313 8989 **Teletypewriter** 13 36 77 gww.com.au

Greater Western Water has fallen short of the standards our customers expect and deserve, and those we hold ourselves to. We are committed to strengthening our approach and ensuring the protection of personal information remains central to everything we do.

Yours sincerely,

The Hon. Lisa Neville
Chair
Greater Western Water