GUARDING YOUR DATA: ENSURING SAFE CROSS-BORDER TRANSFERS OF PERSONAL INFORMATION

Category: IT Law,Privacy Law and POPIA,Technology Law
written by Tshimangadzo Nengovhela | September 2, 2025



In today's digital age, the global exchange of Personal Information has become a common practice, enabling businesses and individuals to connect across borders. However, with this increased flow of data comes a critical responsibility: ensuring adequate levels of data protection. As organisations transfer Personal Information internationally, the risks associated with data breaches, privacy violations, and regulatory non-compliance rise significantly. This article explores the importance of implementing robust data protection measures during transborder data transfers. It highlights the need for accountability, transparency, and adherence to international standards to safeguard individuals' privacy rights.

Who is and isn't allowed to transfer Personal Information about a Data Subject to a third party located in another country?

According to Section 72 (1) of the Protection of Personal Information Act ("**POPIA**"),[1] a Responsible Party in South Africa cannot transfer personal information about a Data Subject to a third party who is a foreign country unless:

1. The third party receiving the information is governed by a law, binding corporate rules, or an agreement that offers an adequate level of protection;[2]
2. The Data Subject provides consent for the transfer;[3]
3. The transfer is necessary for fulfilling a contract between the data subject and the Responsible Party, or for implementing pre-contractual measures based on Data Subject's request;[4]
4. The transfer is essential for concluding or executing a contract made in the Data Subject's

interest between the responsible party and a third party;[5]
5. The transfer benefits the Data Subject;[6] and
6. If obtaining the Data Subject's consent for the transfer is not reasonably practicable, but if it were feasible, the Data Subject would grant it.[7]

What obligation does the Responsible Party have when transferring Personal Information to another country?

The Responsible Party must ensure that there is Adequate Level of Data Protection when transferring Personal Information to another country. An Adequate Level of Data Protection is outlined in Chapter 3 of POPIA. The 8 Conditions for Lawful Processing of Personal Information are as follows:

1. The first Condition is Accountability. The Responsible Party must ensure that conditions for lawful processing are met.[8]
2. The second Condition is Processing limitation, which deals with the Lawfulness of processing,[9] Minimality,[10] Consent,[11] Justification and objection, and Collection directly from Data Subjects.[12]
3. The third Condition is Purpose specification and The Retention and restriction of records. Personal Information must be collected for a specific, explicit and lawful purpose.[13] The Data Subject must be informed of this purpose. Furthermore, the Records of Personal Information should not be kept longer than necessary to fulfil the purpose for which they were originally collected or later processed.[14]
4. The fourth Condition is Further processing limitation. Any further processing of Personal Information must align with or be compatible with the purpose for which it was originally collected.[15]
5. The fifth Condition is Information quality. A responsible party should take appropriate measures to ensure that Personal Information is complete, accurate, not misleading, and updated when necessary.[16]
6. The sixth Condition is Openness. A responsible party must keep records of all processing activities it oversees.[17] If Personal Information is collected, the responsible party should take reasonable steps to ensure that the data subject is informed.[18]
7. The seventh Condition is Security Safeguards. POPIA mandates that organisations implement appropriate security safeguards to protect personal information from loss, damage, unauthorised access, or disclosure.[19] This includes both technical measures, like encryption and firewalls, and organizational measures, such as training staff and establishing access controls. Organisations must also regularly assess and update these safeguards to ensure they remain effective.
8. The eighth Condition is Data Subject Participation, POPIA emphasizes the importance of data subject participation by granting individuals specific rights regarding their Personal Information. Data subjects have the right to:
9. **Access**: Request access to their personal information held by organisations.[20]
10. **Correction**: Request the correction of inaccurate or incomplete information.[21]
11. **Objection**: Object to the processing of their personal information under certain circumstances.
12. **Withdrawal of Consent**: Withdraw consent for processing, where applicable.

These rights empower data subjects to be actively involved in how their personal information is handled and ensure transparency in data processing activities. Organisations are required to inform data subjects about these rights and facilitate their exercise.

When a foreign country lacks adequate protection measures, POPIA stipulates that Personal Information may not be transferred to that country unless specific conditions are met. This includes ensuring that the data subject's rights are adequately protected or that appropriate safeguards are in place to mitigate the risk of inadequate protection. Organisations must assess the risks and may need to implement additional measures to ensure compliance with POPIA when transferring personal information internationally.

In conclusion, it is essential for a responsible party to prioritize the protection of Personal Information when transferring data to a foreign country. Ensuring that adequate safeguards are in place not only complies with legal requirements under POPIA but also fosters trust with data subjects. By carefully assessing the protection levels of the receiving country and implementing necessary measures, organisations can mitigate risks and uphold the integrity of personal information. Ultimately, a proactive approach to data protection demonstrates a commitment to privacy and enhances the overall security framework, benefiting both the organisation and the individuals whose data is being handled.

---

[1] Section 72 (1) of the *Protection of Personal Information* Act 4 of 2013.

[2] Section 72 (1) (a) of the *Protection of Personal Information* Act 4 of 2013.

[3] Section 72 (1) (b) of the *Protection of Personal Information* Act 4 of 2013.

[4] Section 72 (1) (c) of the *Protection of Personal Information* Act 4 of 2013.

[5] Section 72 (1) (d) of the *Protection of Personal Information* Act 4 of 2013.

[6] Section 72 (1) (e) of the *Protection of Personal Information* Act 4 of 2013.

[7] Ibid.

[8] Section 8 of the *Protection of Personal Information* Act 4 of 2013.

[9] Section 9 of the *Protection of Personal Information* Act 4 of 2013.

[10] Section 10 of the *Protection of Personal Information* Act 4 of 2013.

[11] Section 11 of the *Protection of Personal Information* Act 4 of 2013.

[12] Section 12 of the *Protection of Personal Information* Act 4 of 2013.

[13] Section 13 of the *Protection of Personal Information* Act 4 of 2013.

[14] Section 14 of the *Protection of Personal Information* Act 4 of 2013.

[15] Section 15 of the *Protection of Personal Information* Act 4 of 2013.

[16] Section 16 of the *Protection of Personal Information* Act 4 of 2013.

[17] Section 17 of the *Protection of Personal Information* Act 4 of 2013.

[18] Section 18 of the *Protection of Personal Information* Act 4 of 2013.

[19] Section 19 of the *Protection of Personal Information* Act 4 of 2013.

[20] Section 23 of the *Protection of Personal Information* Act 4 of 2013.

[21] Section 24 of the *Protection of Personal Information* Act 4 of 2013.