PERSONALDATA.IO

Policy Report

Recommendations to ensure the exercise of data access and portability rights in Kenya and Nigeria, while improving its practicality in a globalised labour market

April 2025

Authors: Jessica Pidoux, Nawale Lamrini, Sofia Kypraiou, Jacob Gursky, Paul-Olivier Dehaye (PersonalData.IO).

This report results from the project “Data4Mods: Content Moderators’ Collective Power through Data” developed by PersonalData.IO and the African Content Moderators’ Union (ACMU): Kauna Malgwi Ibrahim, James Oyange, Mophat Okinyi, Richard Mathenge, and Sonia Matete.

The project was funded by the Data Empowerment Fund (between OpenCollectives and Omidyar Network) between 2024 and 2025.

Context

The NGO *PersonalData.io* is dedicated to “making data rights individually actionable and collectively useful.” Our aim is to use personal data rights to make the digitalisation of society more legible and understandable. While we are convinced that this is achievable—and that the key lies in the **collective exercise** of the right of access—we have gathered evidence from various platforms (Uber, Tinder, Bumble, Deliveroo, etc.) showing that, in practice, **individual data rights are still far from being truly actionable** for data subjects. As a result, we have had to focus on the **individual exercise** of these rights, in order to defend their **fundamental relevance and enforceability**. Nevertheless, our work continues to contribute to a broader shift toward the **collective use** of data rights.

Since 2017, we have supported platform workers—primarily drivers, food-delivery couriers, and more recently, content moderators—in exercising their data rights. These workers are, by definition, **data subjects** of the platforms they work through, and often also function as **employees**, even when their legal status as workers is undefined or contested (independent contractor, employee, etc). As data subjects, they frequently encounter **obstacles** when trying to reach the appropriate data protection services. As workers, they often **cannot identify or contact their actual employer or platform**, and they lack the **legal tools and access to information** needed to fully understand how their working conditions are being

shaped—and potentially exploited—by **technological systems that collect and process their personal data**.

In ongoing work in Europe, PersonalData.IO has helped hundreds of Uber drivers in recovering their personal data from Uber, expanding the scope of transparency imposed on Uber, helped escalate those matters to relevant data protection authorities (leading to fines of 10s of M of EUR), and finally helped analyse this data to assist workers in their legal fight around their status as workers and just compensation for their work.

PersonalData.IO pushes the political agenda of a uniform view of data subjects as empowered actors in relation to data as part of their work product, regardless of their sector of activity. We therefore seek to foster a more uniform view of data work, its consequences, and counter powers, highlighting for instance parallels between Uber work and white-collar work in text editors, assisted by AI.

The **African Content Moderators' Union (ACMU)** represents content moderators and data labellers across Africa, advocating for improved working conditions and mental health support. Together, PersonalData.IO and ACMU launched the Data4Mods project—*Content Moderators' Collective Power through Data*[1]—with support from the **Data Empowerment Fund**[2]. Data4Mods investigates and maps the content moderation and data labelling industry across Africa, aiming to **empower workers to exercise their data rights and critically analyse their own personal data.** This project was quickly launched thanks to a strong alignment between the ACMU's and PersonalData.IO's visions on worker empowerment. The rapid expansion of the AI industry, bolstered by growing governmental investment, relies on **human labour for content moderation and data labelling**—tasks essential for training machine learning models and filtering harmful or inappropriate content online. This work involves **manually reviewing images, videos, and text**, or annotating datasets to help algorithms make sense of the world.

These processes generate vast amounts of personal and behavioural data, and often involve **surveillance practices of the worker performing this type of work**, with data flowing from **global South workers to servers and companies based in the global North**. These skilled workers are typically[3] based in countries such as Kenya, Nigeria, the Philippines, Venezuela, and India, and are employed by outsourcing companies headquartered primarily in the Global North—including Europe, North America, and the United Arab Emirates. Through these intermediaries, they ultimately serve major tech companies such as Meta, OpenAI, Google, TikTok, and others, which are also primarily based in the Global North.

Behind these **invisible work flows and global data flows** are thousands of workers who perform **low-paid**, precarious digital labour, often **under intense working hours and exposed to psychologically harmful content.** Employed through outsourcing firms and intermediaries, they are frequently denied formal labour protections, health support, and transparency about how their data (personal and produced for work) are used. After being

[1] https://personaldata.io/en/data4mods/
[2] https://dataempowerment.fund/#initiatives
[3] We also observe a trend of skilled data workers being employed in the Global North to provide specialised annotations, for instance through companies such as outlier.ai.

fired, they are also discriminated against in other similar companies for organising collectively[4].

In this context, **data rights** offer a promising legal tool to **expose working conditions, recover personal data, and demand accountability** from tech companies. When exercised collectively, these rights can support efforts to improve transparency, challenge algorithmic exploitation, and strengthen **labour protections across borders**.

Scope

This policy report provides recommendations on how to ensure data subjects' rights are respected, by gathering evidence on the assessment of the practicality of the rights' exercise of access and portability in two main outsourcing companies in Africa: Teleperformance and Sama.

Teleperformance, formerly known as Majorel, is a major multinational business process outsourcing (BPO) company that provides customer service, content moderation, and other digital services. Its clients include large tech platforms such as TikTok, and Meta. As part of this project, three workers in Kenya submitted Subject Access Requests (SARs) to Teleperformance.

Sama is a data annotation and AI training company that offers services to major tech firms, including Meta also, Sony, gm, Gettyimages, Verizon, precision AI, Swift, Walmart, Microsoft, firs, eBay, nasa, Siemens[5]. It employs a large workforce engaged in tasks such as content moderation and data labeling. Under this project, two workers in Nigeria submitted SARs to Sama.

This document is intended for policymakers and data protection authorities in Nigeria and Kenya, as well as in Europe to enforce a fundamental right, Art. 8 of the EU Charter of Fundamental Rights and the respect of Art. 15 and 20 of the GDPR. More broadly, it should serve as a lesson of how both African and European citizens are affected by the fragility of cross-continental jurisdictions in which global data flows are being embedded.

It should be noted that **the issue of access to the right to data protection is reinforced in this context by the fundamental rights of individuals to respect and dignity, particularly in relation to their rights as workers.**

However, a major challenge has emerged for the NGO in pursuing its initiatives: the recognition by these companies of European data protection law, namely the General Data Protection Regulation (GDPR), officially known as Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC.

---

[4] https://www.business-humanrights.org/en/latest-news/kenya-lawsuit-alleges-discriminatory-hiring-practices-after-meta-reportedly-directed-majorel-not-to-hire-former-sama-content-moderators/ [Last accessed 01.04.2025]

[5] https://www.sama.com/case-studies [Last accessed 01.04.2025]

Although the Kenyan data protection legislation—'The Data Protection Act of 2019'—transposes key principles of the GDPR, the companies in question have refused to acknowledge the applicability of the GDPR, arguing that its territorial scope is limited to European citizens. However, we were able to demonstrate, firstly, that the transfer of data to third parties located within the European Union results in the de facto application of the GDPR, as provided under Article 3(1), and secondly, that these entities, acting as data controllers, have their registered office, place of business, or a permanent establishment within the European Union.

Moreover, established case law from the Court of Justice of the European Union (CJEU) has consistently confirmed that the data processing activities of a controller or processor established outside the Union may be inextricably linked to the activities of a local establishment situated in the territory of a Member State. These rulings and analyses have validated the applicability of Union law, even where the local establishment does not, in practice, play any role in the processing itself.

Furthermore, regarding the targeting criterion raised by these companies, it must be recalled that Article 3(2) of the GDPR does not limit its scope based on the nationality or residence of the data subject. While it is true that the data subjects were not physically present in any EU Member State, their activities and personal data were nonetheless processed within the Union.

Article 8(1) of the Charter of Fundamental Rights of the European Union affirms that "Everyone has the right to the protection of personal data concerning them."

Exercising Rights

The European General Data Protection Regulation (GDPR) provides for two forms of data restitution that we have focused on:

Access (Article 15): This covers personal data relating to the data subject, including data provided by the individual, data supplied by third parties, and data inferred by the platform.

More broadly, the exercise of the right of access covers one of the most important rights of the GDPR and requires data controllers to provide all the following information:

" Article 15 of the GDPR - Right of access by the data subject :

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing; (b) the categories of personal data concerned;
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the controller the rectification or erasure of personal data, or the restriction of the processing of personal data relating to the data subject, or the right to object to such processing;
f) the right to lodge a complaint with a supervisory authority;
g) where the personal data are not collected from the data subject, any available information as to their source;
(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

1. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
2. The controller shall provide a copy of the personal data undergoing processing. The controller may require the payment of reasonable fees based on administrative costs for any additional copies requested by the data subject. Where the data subject makes the request by electronic means, the information shall be provided in a commonly used electronic form, unless otherwise requested by the data subject.
3. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others."

Portability (Article 20): This applies to personal data relating to the data subject which they have provided themselves.

<u>The right to portability covers the following actions:</u>

' Article 20 of the GDPR - Right to data portability

1. Data subjects shall have the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
(b) the processing is carried out by automated means.

1. Where the data subject exercises his or her right to data portability pursuant to paragraph 1, he or she shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
2. The exercise of the right referred to in paragraph 1 of this article shall be without prejudice to Article 17. This right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

3. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of third parties.
4. The right referred to in paragraph 1 does not infringe the rights and freedoms of third parties. ‘

Teleperformance, headquartered in Paris with offices across Europe and globally, and Sama, headquartered in San Francisco with offices in the Netherlands, are subject to the GDPR when accessing workers' personal data due to their presence in the EU (for more details see our map [https://personaldata.io/en/bpo-map/]). This also demonstrates the potential of tracing data flows to enhance protections for workers in countries where data protection frameworks are weak or nonexistent. This raises important questions for further investigation regarding how data rights can be leveraged to strengthen labour rights, particularly in efforts to improve working conditions in content moderation. The concept of interlegality—the interaction of multiple legal frameworks—has already proven beneficial in litigation cases and labour rights claims, as seen in legal actions involving Uber drivers[6].

Methods used

Requests were made through GDPR letters written in support with PersonalData.IO’s Data Protection Officer (DPO). They were sent directly to the company’s DPO. However, Teleperformance constraints data subjects to make data access requests via their online portals without providing a contact person.

The process took place over an extended period due to companies **not providing data immediately**, requiring continuous follow-ups, and the process imposed by Teleperformance via their online form which did not allow data subjects to reply directly to their answers.

Priorities for Enforcing Personal Data Protection

Priority 1: Facilitate the Practical Exercise of Data Subject Rights and the Applicability of GDPR to Cross-Border Data Processing

Ensure that multiple channels for contact to data protection services are available, accommodating varying levels of technical literacy—such as email, postal addresses, specially when companies impose online forms. When online forms are imposed (as in the case of Teleperformance), they must be accompanied by a valid contact email address and ensure workers promptly get an email receipt of their entire request, with a timeline for response.

[6] Li, W., & Toh, J. (2022). Data Subject Rights as a Tool for Platform Worker Resistance : Lessons from the Uber/Ola Judgments. In *SSRN Electronic Journal* (Vol. 15). https://www.ssrn.com/abstract=4306868

One data subject was able to contact Teleperformance, which provided a procedure that included a broken URL: “In order to place a Data Subject Access Rights request, you must contact your local HR or go to https://www.teleperformance.com/en-us/data-privacy-information-and-inquiries/[7] click on submit a subject rights request and fill out the form. We hereby inform you that once you can define the scope of your Data Subject Access Rights, the Privacy Office will be glad to start processing it immediately.” As a result, the data subject was unable to access the designated form through the provided link and was forced to independently search for the correct procedure to exercise their rights. This lack of a functional access point created an additional barrier to the effective exercise of data protection rights under the GDPR. In 2022 the European Data Protection Board published guidelines about design patterns that infringe upon data subject rights. In this framework, according to the European Data Protection Board (EDPB) guidelines, the missing link above is an example of a “dead end”, and obstructs the data subject’s rights to transparency and easy access to information under the GDPR and similar frameworks[8].

Teleperformance’s online form constrains the exercise of rights by design. Indeed, the form offers only predefined options, making it impossible for data subjects to simultaneously request access and data portability. As a result, data subjects are forced to repeat the process, creating an undue burden and discouraging the effective exercise of their rights. Furthermore, Teleperformance form is connected to a generic, no-reply email address, which prevents data subjects from following up when responses are incomplete or when requests are closed without adequate justification. Consequently, data subjects must return to the online form and submit a new request, further complicating and delaying the exercise of their rights. This can be considered an example of the “longer than necessary” deceptive design pattern as described by the EDPB.

Moreover, in correspondence with a data subject, Teleperformance asserted that the General Data Protection Regulation (GDPR) was not applicable to the processing of their data, stating: “We wish to clarify the applicable law to your processing. As a Kenyan citizen, whose data was being processed in Kenya, and whose processing was being done by one of our subsidiaries in Kenya, for the purpose of employment contractual obligation, the processing of your data is subject to laws of Kenya and not the GDPR.”

This interpretation is problematic and potentially non-compliant with the GDPR. While the data subject is indeed located in Kenya and the processing is carried out by a local subsidiary, Teleperformance operates offices and services within the European Union. In addition, the first access requests have revealed that data transfers with third parties were carried out on an ongoing basis with these companies. Consequently, the data flows indicate that processing operations were carried out within the EU and were also transferred outside the EU, without adequate protection measures being guaranteed for the data subjects. As indicated in our analysis of the scope (above), the GDPR is intended to apply not only to

[7] (Last accessed on 21.03.2025, see print screen in Annex)
[8] European Data Protection Board, “
Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them”, URL:
https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en, Last updated 24 February 2023.

processing carried out within the EU, but also to the processing of personal data outside the EU where: the controller or processor is established in the EU and the processing relates to its activities (Article 3(1)); or the data processing involves the offering of goods or services to individuals in the EU or the monitoring of their behaviour (Article 3(2)).

Finally, table 1 with Subject Access Requests (SARs) response delays highlights significant discrepancies in how data controllers handle identity verification and subsequent data provision. For instance, Teleperformance took up to 53 days to provide an initial data response following identity verification, far exceeding the one-month deadline mandated by the GDPR. Similarly, Sama responded only after 36 days in two separate cases. The validity of an identity is not systematic and it should not extend over an unreasonable period of time, which sometimes lasts one month—the mandatory duration of a response—except in cases where legitimate reasons are clearly communicated to the data subject, thereby extending the response time to a maximum of three months. Whatever the situation, the person must be informed of the consequences within a maximum of one month. These delays suggest potential non-compliance with the right of access, particularly where additional data responses are delayed or entirely absent, such as the 65-day delay observed in one of Teleperformance's cases.

Table 1: SARs' Response Delays

Who is the data collector (controller)?	Who requested the data?	Delay to Identity Verification (Days)	Delay to Initial Data Response (Days)	Delay After Identity Verification (Days)	Delay to Additional Data Response (Days)
Teleperformance	Person 1t	11	15	4	
Teleperformance	Person 2t	4	53	49	
Teleperformance	Person 3t	1	27	26	65
Sama	Person 1s	7	36	29	
Sama	Person 2s	7	36	29	

Consequently, it is required to conduct further investigations into this type of cases where GDPR may be wrongly excluded from applicability, especially in sectors involving transnational labour outsourcing or remote workforce management. It is necessary to enforce the application of GDPR to multinational companies processing data of non-EU workers where there are cross-border data flows involving EU-based entities, promoting harmonised enforcement to prevent regulatory loopholes that allow companies to circumvent GDPR obligations through jurisdictional fragmentation. Moreover, international cooperation mechanisms can help to uphold data subject rights globally where EU-based entities are involved in data processing, ensuring that identity verification processes do not unreasonably delay access rights, reaffirming that responses to Subject Access Requests must be provided within one month, as required by the GDPR, unless a justified extension is clearly communicated.

Priority 2: Transparency on Types of Data Collected and Recipients of Personal Data in Privacy Policies

Ensure that privacy policies are comprehensive, up-to-date, and easily accessible. Privacy policies are one of the primary tools enabling data subjects to understand their rights and how their personal data is collected, processed, and shared.

Currently, **neither Teleperformance nor Sama provide details regarding the categories of personal data collected or the list of data recipients**. Teleperformance does not have a dedicated privacy policy page. Among the available links—Cookie Settings, Website Privacy Notice, Codes and Policies, Legal Statement—the page most likely to host the privacy policy (Website Privacy Notice) leads to a broken link: https://umbraco13.dev.ontp.app/footer/website-privacy-notice/ (last accessed 21.03.2025; see screenshot in Annex). Sama's privacy policy is accessible at https://www.sama.com/privacy-policy#iii-how-we-use-your-personal-data (last accessed 21.03.2025), but it lacks complete information. Requiring data subjects to navigate this complicated list of policies in order to understand their data rights is another example of a "Privacy Maze" deceptive design pattern described by the EDPB.

Priority 3: Proportionality and Compliance with Deadlines in the Identification Process of Data Subjects

Identity verification is a necessary step for data controllers to ensure that personal data is transmitted to the correct data subject. However, it is necessary to ensure that this process must remain proportionate, consistent, and compliant with data protection regulations.

In our investigation, Teleperformance demonstrated an **inconsistent approach to verifying the identity** of the three data subjects who exercised their rights in this project, despite all following the same request procedure. Two data subjects were asked to provide a copy of their national ID, while the third was required to submit significantly more detailed information, including:

- **Email ID** used when applying for a job at Teleperformance
- **Name of the entity** the job was applied for (e.g., Majorel, Teleperformance, Alliance One, TLS Contact, etc.)
- **Location of the office** for which the job was applied
- **Name of the project/department** (if previously associated with Teleperformance or Majorel), along with the name of the **previous Manager/Team Leader**
- **Relationship with the concerned entity**
- **Name of the former manager/supervisor**

Additionally, Teleperformance imposed a strict **7-day response deadline** for providing the requested information: *"Please reply with the additional information as soon as possible. If we do not receive a response within 7 days, we will notify you that the case is closed."* This arbitrary variation in identity verification requirements, combined with a rigid deadline,

creates an unnecessary burden on data subjects and may hinder the effective exercise of their rights under the GDPR.

Sama maintained a consistent approach in both Subject Access Requests (SARs) by requiring data subjects to complete a form and submit a copy of their identity document. The request stated: *"Please fill out the attached form, ensuring that all required information is provided. The duly completed form should be accompanied by a copy of your ID card or passport that corresponds with our employment records for the purpose of verifying your identity."*

However, the form served as a means to **override the initial request** and require the data subject to submit their request again, specifically detailing the exercise of their data access and portability rights. This occurred despite the data subject having already submitted a detailed letter explicitly exercising these rights in accordance with the GDPR. By disregarding the original request and imposing a mandatory form submission, Sama created an additional procedural hurdle, delaying or obstructing the effective exercise of rights if the person did not fill in the form completely. For reference, the form fields can be found in the Annex.

Inconsistent identity verification on a rigid deadline, overriding requests, and providing data subjects with inconsistent ways to exercise are examples of the "inconsistent interface" and "conflicting information" deceptive design patterns as described by the EDPB.

Priority 4: Completeness of Personal Data Collected and Transmitted to Data Subjects, Including Data Processing Information

Companies are required to be transparent on data collection processes, i.e. to provide complete and comprehensive information on the personal data they collect about data subjects, including who it is shared with and for what purposes. However, in our investigation companies have proven to be unreliable in disclosing complete, consistent and accurate data.

During the Subject Access Request (SAR) process, data subjects requested access to all their personal data. However, the **responses varied significantly within the same company**, ranging from no data being provided to only minimal information. In cases where a more substantial amount of data was transmitted, **some entries were deleted** from the files (i.e. a performance rate, a DNA page and payslips for the entire working period were not provided). Additionally, **inconsistencies** were observed, as some data subjects received less data than others, despite having similar profiles and roles within the company.

Teleperformance initially responded to one data subject by providing only a general document outlining their **"Global Retention Policy"** instead of the requested personal data. Following a second request—this time submitted through their mandatory online form—this data subject, along with two others, received a link to a platform where they could **access partial personal data**, specifically **payslips**.

However, two of these data subjects were no longer employed by the company and had lost access to their login credentials, preventing them from retrieving any data. The third data subject managed to log in but found that the **payslips were not downloadable**, further restricting their ability to obtain and use their personal data.

It is important to highlight that, despite the **incompleteness** of the data transmitted, Teleperformance explicitly confirmed that they **retain employment data**: *"In accordance with the Employment Act of Kenya, which requires that employment data is retained for five years post-employment termination, we have your employment data in our records."*

Furthermore, for one data subject, Teleperformance **acknowledged holding significantly more data** than what was actually provided. While this data subject received only **three files**, there was no systematic provision of the same files to the other two individuals who submitted similar requests. A detailed list of the data Teleperformance admitted to holding, compared to what was actually transmitted, can be found in the Annex.

Sama provided more detailed personal data compared to Teleperformance, including a full list of personal data documents (see Annex). However, inconsistencies were identified across the two data subjects, despite both having gone through the same request process.

Key discrepancies include:

- Missing data processors: One data subject received this information, while the other did not.
- Signed offer letter: Provided to one data subject but missing for the other.
- Contract completeness: One data subject received all pages and articles, while the other received an incomplete version.
- Payslip inconsistencies: One subject received only a partial set of payslips, with some months missing, and only one year fully provided.
- Performance rating changes: A subject's rating on a 0-10 scale was changed—one was rated 0, yet the record indicates an increase in salary given the rate.
- Personal document discrepancies: While one subject received both the contract and the signed offer letter, the other only received the contract.
- Missing personal information documents: One data subject received a passport copy, while the other did not.

Moreover, we explicitly requested that data controllers disclose the **recipients of personal data** concerning the data subjects. However, the responses were **limited and inconsistent**, with only **one to four entities** being mentioned—despite **multiple follow-up requests** (at least three in each case). This **incomplete disclosure** contrasts with the accounts of data subjects, who are aware that their data has been processed by a **wider range of entities**.

Teleperformance disclosed only one recipient to a data subject: **ROEDL & Partner Schweiz. Sama** disclosed only the following entities to a data subject: **Ministry of Foreign Affairs in Kenya** – for work permit processing (*information shared: names and passport details*), **Ministry of ICT** – also for work permit processing (*information shared: names and passport details*), **Kenya Revenue Authority, NSSF, and NHIF** – for statutory reporting (*all required employment-related information*), **Palbina (a travel agency)** – for booking flight

details provided by the company. (*Sama noted that this vendor signed a Non-Disclosure Agreement (NDA) prohibiting further data sharing with third parties*).

These discrepancies reveal a **lack of transparency and consistency** in how data controllers disclose both the types of personal data collected and the third parties with whom it is shared. In several cases, data subjects were able to identify additional recipients not mentioned in the companies' responses, raising concerns about the **reliability and completeness** of those disclosures. The inconsistencies observed in Teleperformance's and Sama's responses also point to a **lack of standardisation** in data handling practices, raising questions about the accuracy of their responses and respect of data rights. It is therefore essential that companies provide a **complete and accurate list** of personal data categories and data recipients.

Transparency is not only a **legal obligation** under **GDPR Articles 13 and 14**, but also a necessary step toward **mapping data flows between European and African outsourcing companies**. This mapping is critical to understanding **transnational data processing chains**, identifying **accountability gaps**, and promoting **responsible data governance across jurisdictions**. One alternative is to **conduct technical audits on data collection** and processing practices of these companies to ensure compliance and accountability.

Conclusion

This policy report highlights violations of personal data protection regulations, and fundamental rights, serious and systemic shortcomings in how outsourcing companies, such as Teleperformance and Sama, handle personal data of data subjects (i.e. their employees)—particularly in cross-border contexts involving European and African operations. While transparency is a core obligation under GDPR Articles 13 and 14, our findings show a clear pattern of **non-compliance, procedural obstruction, and selective disclosure**, which undermines the ability of workers to exercise their data protection rights effectively.

Despite GDPR's extraterritorial reach, companies applied the regulation inconsistently, at times claiming it applies only to EU residents while still responding partially to requests. Data provided was often **incomplete or selectively redacted**, omitting crucial elements such as **geolocation data, complete payslip histories, and the identities of third-party data processors**. In some cases, the **Non-Disclosure Agreements (NDAs)** shared were missing essential clauses, raising questions about internal data governance and accountability.

Procedural barriers further obstructed access. Companies imposed **strict and arbitrary deadlines**, required **excessive identity verification**, and relied on **non-functional online forms or login systems** that delayed or prevented data access. This process, rather than facilitating the right to access, became a mechanism of **exclusion and control**.

Non-compliance with the GDPR's **30-day deadline for responding to SARs** was widespread. Several companies failed to provide a complete response within the legal timeframe, and offered little to no justification for these delays. In other cases, they cited **security-based data deletion policies** while simultaneously acknowledging the collection

of sensitive material such as **images, videos, religious affiliation, and vaccination records**, without ensuring proper safeguards or legal bases for such processing.

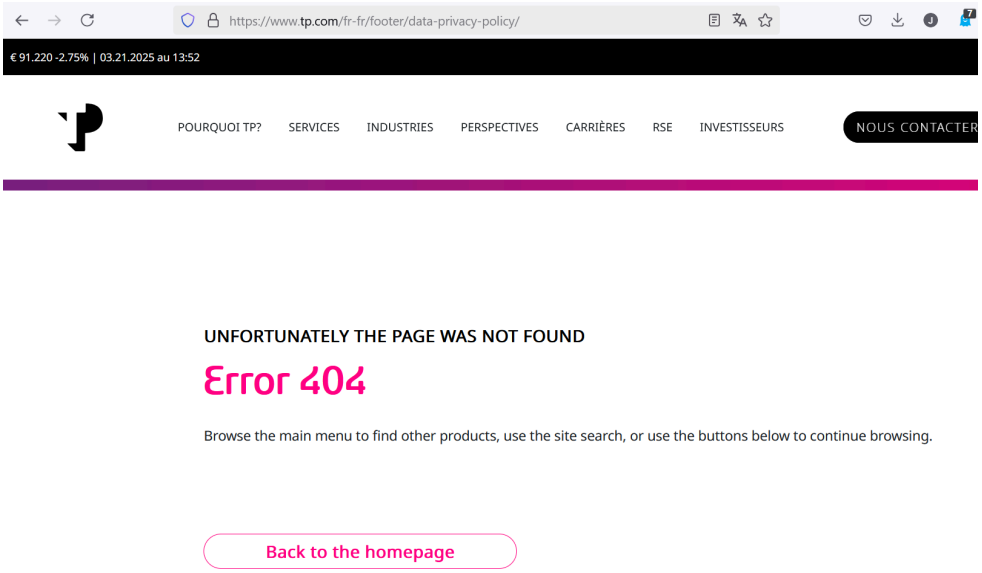
The **incomplete responses to SARs** raise significant concerns about the protection of employment-related data. Missing contracts, training certifications, pay slips, and internal communications deprived workers of evidence necessary to verify employment terms or challenge unfair treatment. In one case, a worker's **salary rating** was altered without explanation, suggesting a potential manipulation of performance data.

Despite these challenges, the SAR process enabled workers and their advocates to **gather critical evidence** of data mismanagement and labour rights risks. Access to personal data can empower workers to verify working hours, contest unfair conditions, and expose previously unknown third-party data sharing practices. This underscores the **potential of data rights as a tool for labour empowerment**, particularly in transnational digital economies.

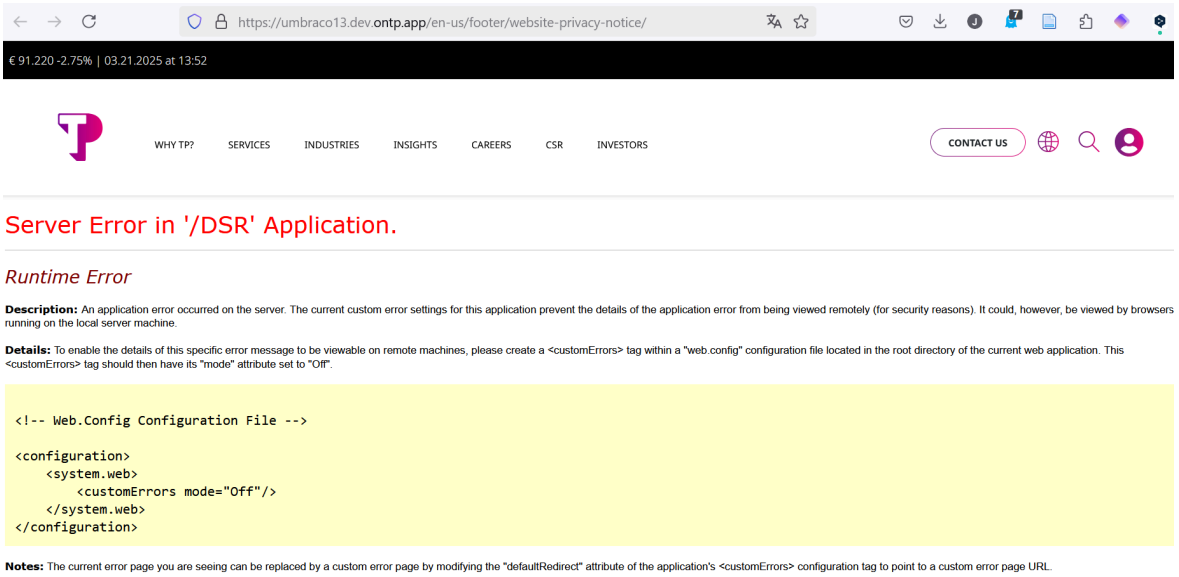
To move forward, **technical audits** and **legal enforcement mechanisms** must be prioritised to hold companies accountable and ensure compliance. Mapping data flows between European and African outsourcing companies is essential to closing the gaps in data governance. Ultimately, advancing data rights is not only a matter of legal compliance—it is a necessary step towards **securing decent work and dignity** for all digital labourers.

Annex.

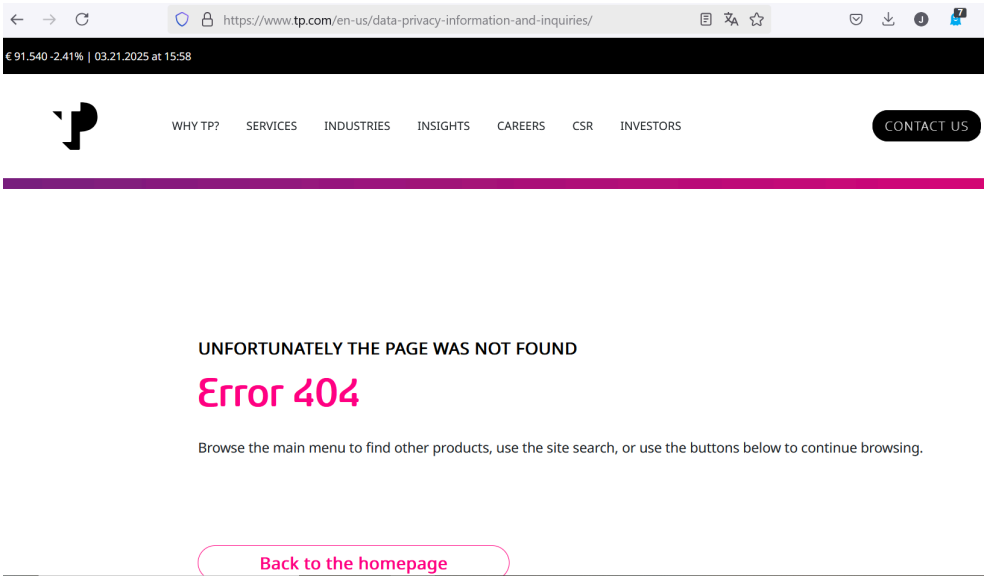
1. Screenshot of Broken Privacy Policy URL1 – Teleperformance



2. Screenshot of Broken Privacy Policy URL2 – Teleperformance



3. Screenshot of Broken Link – Teleperformance Data Request Portal



4. Data Request Form by Sama for Identity Verification

DPG 2[r. 9(2)]

REQUEST FOR ACCESS TO PERSONAL DATA

*Note:(i) Documentary evidence in support of this request may be required.(ii) Where the space provided for in this Form is inadequate, submit information as an annexure(iii) All fields marked as * are mandatory*

A. DETAILS OF THE DATA SUBJECT*(This section is to provide the details of the Data Subject).*Name*:

Name*:		
Identity Number*:		

Phone Number*:		
e-mail address*:		

Name*:

Identity Number*:

Phone number*:

e-mail address:

Relationship with the Data Subject*

Contact Information*

B. DETAILS OF THE PERSONAL DATA REQUESTED*(Describe the personal data requested)*

MODE OF ACCESS

I would like to: *(check all that apply)*

[ ] Inspect the record

[ ] Listen to the record

[ ] Have a copy of the record made available to me in the following format:

[ ] photocopy *(Please note that copying costs will apply)* number of copies required: .....

[ ] electronic[ ] transcript *(Please note that transcription charges may apply)*

[ ] Other *(specify)* .....

C. Delivery Method

[ ] collection in person

[ ] by mail (provide address where different / in addition to details provided above)Town/City: .....

[ ] by e-mail (provide email address where different / in addition to details provided above): .....

DECLARATION

Note any attempt to access personal data through misrepresentation may result in prosecution.☐

I certify that the information given in this application is true.

Signature	Date

5. List of Personal Data Collected by Teleperformance but Not Disclosed

1. Employment Records

- **Full employment contract – Attached**
- **Offer letter – Job description and role responsibilities – Attached**

- **Performance appraisals or reviews** – These are conducted through the system. Once an employee is deactivated from the system, the data is stored in an encrypted format in accordance with our data retention policy.
- **Training records and certifications completed** – These are conducted through the system. Once an employee is deactivated from the system for more than **20 months**, the data is stored in an encrypted format in accordance with our data retention policy.
- **Attendance records (clock-ins, absences)** – Once an employee is deactivated from the system for more than **20 months**, the data is stored in an encrypted format in accordance with our data retention policy.

2. Payroll and Compensation

Access to your **payslip portal** has been provided, which can be accessed using your employee email address. Employees can download all their pay slips, which contain the records below.
The link to the portal is: **https://payroll.hr.majorel.co.ke/login.php**

- **Salary history and pay slips** – Will be obtained from our pay slip processors.
- **Tax records (PAYE, NHIF, NSSF contributions)** – Will be contained in the payslip.
- **Bonuses, commissions, or incentives details** – Will be contained in the payslip.
- **Leave records** (annual leave, sick leave, maternity/paternity leave, etc.) – These are recorded in the system. Once an employee is deactivated for more than **20 months**, the data is stored in an encrypted format in accordance with our data retention policy.

3. Personal Information

This information is contained in the **employee's form** – **Attached**

- **Full name and contact details**
- **National ID details**
- **Date of birth**
- **Marital status and dependents information**
- **Copies of background checks from HireRight**

4. Communication Records

These are considered **confidential** based on our legal and contractual obligations with our clients.

- **Emails, messages, and other forms of communication** between the employee and management/HR.
- **Any internal feedback forms or surveys** participated in.

5. Data Collected for Security Purposes

- Data is **deleted** once an employee is deactivated from the system for more than **12 months**.
- **CCTV footage** at the workplace **West-End offices**.

- **Access logs** (e.g., building entry logs or system access logs).
- **IT usage records** (e.g., browsing history and system usage)

6. List of Personal Data Collected by Sama but Not Fully Disclosed

List (As per documents transmitted):
Payslips
E Permit
Police Clearance Certificate
Passport
Alien ID
Security Bond
Permit (2021-2022)
Work Permit 2019
Work Permit 2020
Passport photo
Employee Emergency Data Form
Dependants capture form
Academic certificates
Candidate information form
Birth certificate
Beneficiary nomination form
Curriculum Vitae
Annual Salary Review Letter
SamaHome Program Agreement
Warning Letter
Work from Home Rules & Guidelines
Confirmation Letter
Homecase Declaration Form
Activity Code Refresher Training Acknowledgement Form
PIP Acknowledgement Form
Redundancy Notice
Redundancy Exit Letter
Contract of employment
Signed offer letter
NDA
Letter of offer
Contract Extension
Education and Employment Check
Criminal Check
Certificate of Verification