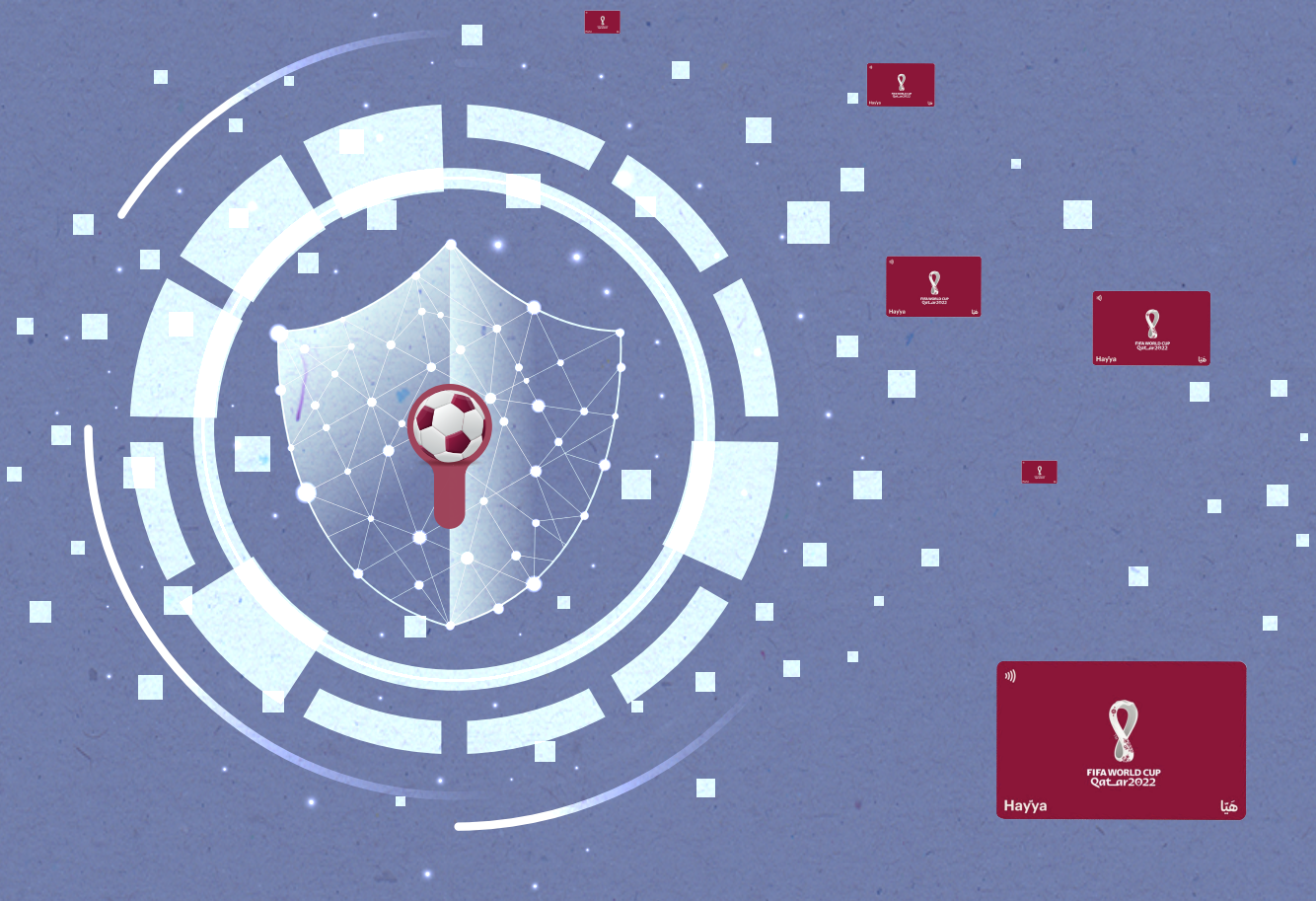
Mandatory App, Opaque Policies:

The Policy Void that Threatens the Privacy of Qatar World Cup Attendees



SMEX

Ranking Digital Rights

Acknowledgements

Aksel Eck, Marianne Rahme, Nathan Sibler, and **Sarah Cupler** are the researchers and authors of this report. **Afef Abrougui** supervised the research and edited the report. **Nourhane Kazak** and **Farah Mokhtareizadeh** provided proofreading support. Design and the illustration are by **Rasha Sayegh**.

This research report is part of **Red Card on Digital Rights**, a campaign launched by **SMEX** and Ranking Digital Rights (RDR) to raise awareness about digital rights during the 2022 FIFA World Cup, taking place in Qatar between November 20 - December 18. The report assesses the privacy policies of Hayya (“let's go” from Arabic), the mandatory registration system for spectators attending the World Cup, and to help those attending and the wider public better understand how Hayya users’ information is handled and protected.

SMEX is a Lebanese NGO that has worked since 2008 to advance digital rights in Lebanon and the Arabic-speaking region through research, campaigns, and advocacy that encourages users to engage critically with digital technologies, media, and networks.

RDR is an independent research program at the policy think tank New America that evaluates the policies and practices of the world’s most powerful tech and telecom companies and studies their effects on people’s fundamental human rights. It is the only organization in the world that produces an open dataset on companies’ commitments and policies affecting users’ freedom of expression and privacy.

www.smex.org

A November 2022 Publication of SMEX.
All errors and omissions are strictly the responsibility of SMEX.

Kmeir Building, 4th Floor, Badaro, Beirut, Lebanon

SMEX

Table of Contents

Key definitions

▪ **Ad targeting rules:** Rules governing what advertising targeting parameters are permitted on the platform.

▪ **Advanced authentication methods:** Involve asking users to provide separate pieces of evidence in combination to access their account—for example, requiring a login password plus a code delivered via a separate email account or text message, an authenticator app, a security token, etc. The methods can be two-factor authentication (2FA) or multi-factor authentication. This authentication should show which devices have access to the account.

▪ **Advertising audience categories:** Groups of users, identified for the purpose of delivering targeted advertising, who share certain characteristics and/or interests, as determined on the basis of user information that a company has either collected or inferred.

▪ **Data breach:** A data breach occurs when an unauthorized party gains access to user information that a company collects, retains, or otherwise processes, and which compromises the integrity, security, or confidentiality of that information.

▪ **Due diligence on government surveillance demands:** Entails the careful review by entities hosting the user information of demands to access that information. Demands should be reviewed for legality (i.e. whether a request comes from the appropriate authority, follows the proper legal process, and is not overly broad, etc.) before a company or entity complies with them.

▪ **Encryption:** This essentially hides the content of communications or files so only the intended recipient can view it. The process uses an algorithm to convert the message (plaintext) into a coded format (ciphertext) so that the message looks like a random series of characters to anyone who looks at it. Only someone who has the appropriate encryption key can decrypt the message, reversing the ciphertext back into plaintext. Data can be encrypted when it is stored and when it is in transmission.

▪ **Grievance mechanism:** It is a mechanism "used to indicate any routinized, State-based or non-State-based, judicial or non-judicial process through which grievances concerning business-related human rights abuse can be raised and remedy can be sought." (Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (2011), p. 27). https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

▪ **Hayya ("Let's go" in Arabic):** It is the mandatory registration system for spectators attending the 2022 World Cup. Spectators attending this year's tournament must obtain a Hayya Card, which they can apply for through the Hayya Portal or App. The card provides spectators with an entry permit into Qatar and access to the stadiums. Throughout the report we also refer to the Hayya program or system, or the Hayya App and Hayya Portal. When we reference the SC's policies, it should be noted that these apply to Hayya as well.

▪ **Inference of user information:** It involves the deployment of "big data" analytics and algorithmic decision making technologies to draw inferences and predictions about the behaviors, preferences, and private lives of its users. These methods might be used to make inferences about user preferences or attributes (e.g., race, gender, sexual orientation), and opinions (e.g., political stances), or to predict behaviors (e.g., to serve advertisements).

▪ **Remedy:** It "may include apologies, restitution, rehabilitation, financial or non-financial compensation and punitive sanctions (whether criminal or administrative, such as fines), as well as the prevention of harm through, for example, injunctions or guarantees of non-repetition. Procedures for the provision of remedy should be impartial, protected from corruption and free from political or other attempts to influence the outcome." (Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (2011), p. 27.)

▪ **Security vulnerability:** A weakness which allows an attacker to reduce a system's information assurance. A vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

▪ **Targeted advertising:** Targeted advertising, also known as "interest-based advertising," "personalized advertising," or "programmatic advertising," refers to the practice of delivering tailored ads to users based on their browsing history, location information, social media profiles and activities, as well as demographic characteristics and other features. Targeted advertising relies on vast data collection practices, which can involve tracking users' activities across the internet using cookies, widgets, and other tracking tools, in order to create detailed user profiles.

▪ **Targeting parameters:** The conditions, typically set by the advertiser, that determine which users will be shown the advertising content in question. This can include users' demographics, location, behavior, interests, connections, and other user information.

▪ **Technical means:** Companies deploy various technologies, such as cookies, widgets, and buttons to track users' activity on their services and on third-party sites and services. For example, a company may embed content on a third-party website and collect user information when a user "likes" or otherwise interacts with this content.

▪ **The Supreme Committee for Delivery and Legacy (also referred to throughout the report as the SC or the Committee):** It was established in 2011 by the Qatari government to deliver the required infrastructure and plan operations for the hosting of the 2022 World Cup.

▪ **Tracking:** Practice by which operators of websites and third parties collect, store, and share information about users' behaviors across domains. In addition to users' movements on a website, personal data such as the IP address can also be collected. The practice may involve using cookies, widgets, and other tracking tools, in order to create detailed user profiles.

▪ **User information:** It is any data that is connected to an identifiable person, or may be connected to such a person by combining datasets or utilizing data-mining techniques. User information may be either collected or inferred. As further explanation, user information is any data that documents a user's characteristics and/or activities. This information may or may not be tied to a specific user account. This information includes, but is not limited to, personal correspondence, user-generated content, account preferences and settings, log and access data, data about a user's activities or preferences collected from third parties either through behavioral tracking or purchasing of data, and all forms of metadata. User information is never considered anonymous except when included solely as a basis to generate global measures (e.g. number of active monthly users).

Introduction

Qatar made history in 2010 by winning the bid to become the first Arab nation to host the FIFA World Cup. It has since spent the last 12 years preparing for the World Cup by investing in new stadiums, an airport expansion, newer and larger highways, 100 new hotels, and a $36 billion metro system. The news of Qatar becoming the World Cup host led to greater scrutiny of the country's human rights record, specifically of its treatment of migrant workers and LGBTQI+ individuals. Qatar has spent an estimated $220 billion in new construction and over two million migrant workers have worked to realize this ambition under deplorable conditions.

Amnesty International revealed that the exploitation of migrant workers through forced labor, unpaid wages, and long hours is how Qatar has achieved its goals. According to Human Rights Watch (HRW) "several thousand" workers who migrated to the country to work on World Cup infrastructure since 2010 have died. It is unclear how many of these deaths were directly linked to construction sites, but HRW attributed many of these deaths to "heat and poor working and living conditions."

HRW has also exposed violations of LGBTQI+ rights, with several individuals facing arbitrary arrest and physical and sexual assault while in police custody. Various football team players from the Netherlands, Norway, Germany and Australia have all protested against these violations of human rights, with more teams expected to follow suit as the group stages begin. The Qatari response has ranged from organizers condoning the actions of the state saying "no country is perfect" but also praising the footballers for using their voice for important matters, to the country's ruler denouncing these critiques as being part of a "ferocious" and "unprecedented campaign" of double standards that no other host country has faced.

1 Mark Ogden, "Qatar's World Cup preparations: Are the 2022 hosts ready for November?", ESPN, September 20, 2022, https://www.espn.com/soccer/fifa-world-cup/story/4750906/qatars-world-cup-preparations-are-the-2022-hosts-ready-for-this-winter.
2 Minky Worden, "The World Cup is Exciting, Lucrative, and Deadly," Human Rights Watch, August 23, 2022, https://www.hrw.org/news/2022/08/23/world-cup-exciting-lucrative-and-deadly.
3 "Reality Check: Migrant Workers Rights With Two Years to Qatar 2022 World Cup," Amnesty, 2019, https://www.amnesty.org/en/latest/campaigns/2019/02/reality-check-migrant-workers-rights-with-two-years-to-qatar-2022-world-cup/.
4 Minky Worden, "The World Cup is Exciting, Lucrative, and Deadly," Human Rights Watch, August 23, 2022, https://www.hrw.org/news/2022/08/23/world-cup-exciting-lucrative-and-deadly.
5"Qatar: Security Forces Arrest, Abuse LGBT People," Human Rights Watch, October 24,2022, https://www.hrw.org/news/2022/10/24/qatar-security-forces-arrest-abuse-lgbt-people.
6 "Why are football teams protesting against Qatar 2022 World Cup?", Aljazeera, March 28, 2021, https://www.aljazeera.com/news/2021/3/28/why-are-football-teams-protesting-against-qatar-2022-world-cup.
7 Mike Hytner, "World Cup organisers in Qatar respond to Australian players' criticism, saying 'no country is perfect'," The Guardian, October 28, 2022, https://www.theguardian.com/sport/2022/oct/28/world-cup-organisers-in-qatar-respond-to-australian-players-criticism-saying-no-country-is-perfect.
8 Ibid.
9 "Qatar emir slams 'ferocious' campaign against World Cup host," Aljazeera, October 25, 2022, https://www.aljazeera.com/news/2022/10/25/qatar-emir-slams-unprecedented-campaign-against-world-cup-hosts.

Alongside these issues, the Qatar World Cup has ushered in a plethora of technologies. Smart city tech, drones, wearable tech, new navigation apps and the use of facial recognition has been invested in and made available for the Cup. Access to the tournament requires spectators to obtain a Hayya card, which can be obtained through the Hayya Portal or App. Hayya was launched by the Supreme Committee for Delivery and Legacy (SC), tasked with planning and operations for this year's tournament. The Hayya Card provides fans with an entry permit into Qatar, entry into stadiums, fan events and amenities such as free transport and a free sim card with Qatari operator Ooredoo. Fans cannot access any of the stadiums without signing up for a Hayya card. This kind of surge in technology use, especially technology that cannot be opted out of, raises questions as to how spectators' rights related to privacy and data will be protected.

This research uses the Ranking Digital Rights (RDR) methodology to assess the policies and practices of the Hayya app and portal in relation to privacy and protection of user information. The methodology benchmarks companies in the Information and Communication Technology sector (ICT) using a group of indicators that set high but achievable standards for corporate transparency and policies that align with internationally recognized human rights standards.

We evaluate relevant policies and practices of the Hayya App and Portal to help those traveling to Qatar for the World Cup and the wider public better understand how spectators' user information is handled and protected. We compare Hayya's policies with the local law while also outlining where they fall short of RDR standards. Our analysis explores remedies for privacy related grievances, access to and notification of changes to privacy policies, user information collection, sharing, inference, and retention, targeted advertising and tracking, handling of government surveillance, and security. In all areas, Hayya's policies had shortcomings and lacked transparency, which can pose risks to fans' rights to privacy.

10 "Qatar Smart City Project Takes Shape As FIFA World Cup Draws Near," Qatar Tribune, June 22, 2022, https://www.qatar-tribune.com/article/237007/OPINION/Qatar-Smart-City-Project-Takes-Shape-As-FIFA-World-Cup-Draws-Near.
11 "Qatar's ground control on alert for World Cup disasters," France 24, August 12, 2022, https://www.france24.com/en/live-news/20220812-qatar-s-ground-control-on-alert-for-world-cup-disasters.
12 Vas Panagiotopoulos, "Soccer Fans, You're Being Watched," Wired, November 3, 2022, https://www.wired.com/story/soccer-world-cup-biometric-surveillance/.
13 Frequently Asked Questions, Hayya Portal, https://hayya.qatar2022.qa/web/hayya/faqs#553643.
14 "Ooredoo Launches Hayya SIM Enabling FIFA World Cup Qatar 2022™ Fans to Stay Connected FREE of Charge," October 10, 2022, https://www.ooredoo.com/en/media/news_view/ooredoo-launches-hayya-sim-enabling-fifa-world-cup-qatar-2022-fans-to-stay-connected-free-of-charge/.
15 "Methods and Standards," Ranking Digital Rights, https://rankingdigitalrights.org/methods-and-standards/.

Key Findings

- **Access to remedy.** The SC's mechanism to address the privacy concerns of users of the Hayya app and portal is deficient. The mechanism does not seem to cover all the range of possible privacy harms that may emanate from the committee's practices and policies in relation to Hayya. Procedures for providing remedy for privacy-related grievances were not disclosed.

- **Collection, sharing, inference, and retention of user information.** The SC lacks transparency about its collection, inference, sharing, and retention of Hayya users' information, falling short of RDR standards. It is transparent about which user information it collects and how, but does not list all the types of user information it infers and shares, nor its purposes for doing so. Its policy of user information retention is opaque and it is unclear for how long information of Hayya App and Portal users is retained. Finally, users lack control over their information and are only able to access their information in some cases.

- **Targeted advertising and tracking.** The SC provides only limited information about its targeted advertising and tracking practices, despite clearly engaging in them. It permits advertisers to engage in the problematic practice of targeting specific individuals by using their email addresses. Targeted advertising is only off by default "where required by law," and it is not clear if the committee respects user generated signals not to be tracked.

- **Government Surveillance.** Information surrounding surveillance is scarcely provided by the SC. It does not clearly state its process for responding to government demands for user information of its Hayya App and Portal users but mostly offers vague statements that it may disclose information to comply with legal obligations inside and outside Qatar.

- **Security.** Spectors attending the World Cup are in the dark about what measures and policies the SC has in place to protect their information on the Hayya App and Portal. The committee does not disclose whether or not it monitors and limits employee access to user information or if it conducts security audits. It is not transparent about its policy for handling data breaches nor does it disclose tools—such as advanced authentication methods— for users to secure their information.

Methodology

To assess to what extent the Hayya platforms are privacy and security centric, we used selected privacy and security standards from the RDR methodology. First, we reviewed the key policies and conducted a preliminary analysis to identify the areas that are of most relevance and importance in the Qatari context, given the lack of robust data protection legislation and the country's disproportionate surveillance practices.[16]

The key policies are the Privacy Policy[17] , Cookie Notice[18] and Terms of Use[19] of the Supreme Committee for Delivery and Legacy (SC). The committee was established in 2011 by the government to deliver the required infrastructure and plan operations for hosting this year's tournament. Its policies apply to all of its websites and applications, including the Hayya App and Portal, the official Qatar World Cup website (https://www.Qatar2022.qa), and the accommodation portal, which fans have the option to use to book their accommodation in Qatar. In our assessments, we focus on the Hayya App and Portal as some form of interaction with these is required to obtain and access the Hayya Card, which is mandatory for those attending the World Cup.[20] Fans have to apply for the Hayya Card using the Hayya portal (https://www.Qatar2022.qa/hayya/) or Hayya to Qatar 2022 app[21] (which throughout this research, we will simply refer to as the Hayya App). Once approved, the Card is available and can be accessed via the Hayya App. It provides non-resident spectators with an entry permit to Qatar to attend the tournament and all fans with match tickets—residents and non-residents— with access to stadiums. Fans can also use the card to access public transportation for free during the event and plan their journeys using the app.

Based on the preliminary analysis, we decided to assess the Hayya App and Portal in the following privacy areas areas:

Remedy for privacy-related grievances[22] The Hayya App and Portal should have clear and predictable grievance and remedy mechanisms to address users' freedom of expression and privacy concerns.

16 "Submission to the United Nations Human Rights Council, on the Universal Periodic Review for Qatar in 2019," Access Now, 2019, https://www.accessnow.org/cms/assets/uploads/2018/10/Qatar-UPR-Digital-rights.pdf.
17 SC Privacy Policy, Fifa World Cup 2022, https://www.qatar2022.qa/en/privacy-policy.
18Cookie Notice, Fifa World Cup 2022, https://www.qatar2022.qa/en/cookie-policy.
19 "Terms of Use," Fifa World Cup Qatar 2022, https://www.qatar2022.qa/en/terms-of-use.
20 Frequently Asked Questions, Hayya Portal, https://hayya.qatar2022.qa/web/hayya/faqs#553643.
21 "Hayya" in Arabic means "let's go."
22 Privacy elements of the G6a indicator in the RDR methodology, https://rankingdigitalrights.org/index2022/explore-indicators.

Access to and notification of changes to privacy policies [23] The Hayya App and Portal should offer privacy policies that are easy to find and easy to understand and commit to directly notify users when it changes these policies, prior to these changes coming into effect.

User information collection, inference, sharing, and retention The Hayya App and Portal should be transparent about the user information they collect,[24] infer,[25] and share,[26] and for what purposes.[27] Clear retention periods of collected information should also be specified[28] and spectors should be provided with clear options to access[29] and control[30] their information.

Targeted advertising and tracking The SC should disclose its policies governing what type of advertising targeting is prohibited31 and provide options for fans to control the use of their information for targeted advertising.32 It should be transparent about its third-party tracking practices. 33

Government surveillance We expect the SC to provide a clear process for handling government demands for user data34 and should provide data about the numbers of these demands and its compliance rates. 35

Security We expect the SC to disclose information about its institutional processes to ensure the security of its Hayya program.36 It should also publicize a mechanism through which security researchers can report security vulnerabilities37 and a transparent policy on handling data breaches.38 Advanced encryption39 and authentication40 methods should also be deployed.

For the assessment, we followed a simplified version of the RDR research process, which consists of 7 steps and includes a step for sending initial results to companies and accepting their feedback. Given the lack of disclosure and limited scope of this research (in terms of areas and services assessed), we opted only for three steps. In the first step, a primary researcher reviewed the policies and provided their initial assessments. Another researcher reviewed these assessments, after which any disagreements were resolved. Policy research was supplemented with relevant findings from a jurisdictional analysis conducted by RDR.

---

23 Indicators P1a and P2a in the RDR methodology.
24 Indicator P3a in the RDR methodology.
25 Indicator P3b in the RDR methodology.
26 Indicator P4 in the RDR methodology.
27 Indicator P5 in the RDR methodology.
28 Indicator P6 in the RDR methodology.
29 Element 1-4 and 6 of Indicator P8 in the RDR methodology.
30 Elements 1-4 of Indicator P7 in the RDR methodology.
31 Indicator F3c in the RDR methodology.
32 Elements 4-5 of Indicator P7 and 5 of Indicator P8 in the RDR methodology.
33 Element 1-4 of Indicator P9 in the RDR methodology.
34 Indicator P10a in the RDR methodology.
35 A simplified and adapted version of Indicator P11a in the RDR methodology.
36 Indicator P13 in the RDR methodology.
37 Element 1-3 of Indicator P14 in the RDR methodology.
38 Indicator P15 in the RDR methodology.
39 Indicator P16 in the RDR methodology.
40 Indicator P17 in the RDR methodology.

Non-transparent policies keep Hayya users in the dark

Weak mechanisms for addressing privacy concerns

The mechanisms of the Hayya App and Portal to address users' privacy concerns, possible grievances and eventual corresponding remedies, are deficient and a source of concern for users' privacy.

Indicator 1: Remedy for privacy-related grievances

The SC should have clear and predictable grievance and remedy mechanisms to address users' privacy concerns.

Elements:

1. Does the SC clearly disclose it has a grievance mechanism(s) enabling users to submit complaints if they feel their privacy has been adversely affected by the company's policies or practices?

2. Does the SC clearly disclose its procedures for providing remedy for privacy-related grievances?

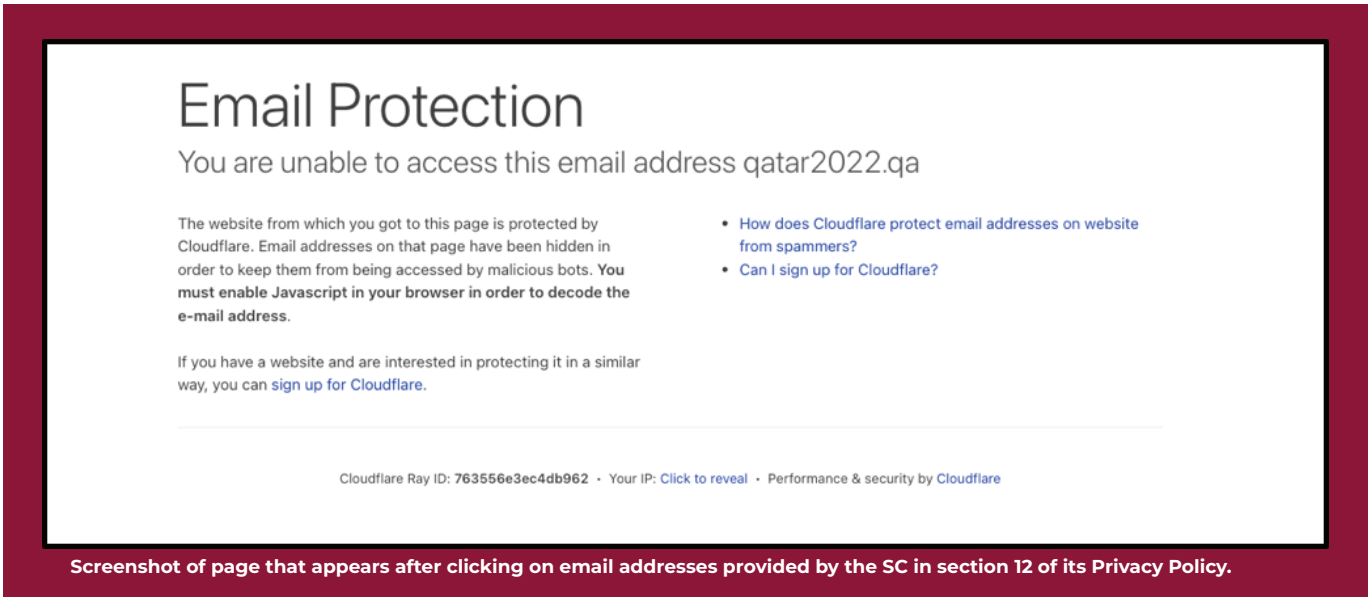
3. Does the SC clearly disclose timeframes for its grievance and remedy procedures?

4. Does the SC clearly disclose evidence that it is providing remedy for privacy grievances?

The mechanism for lodging complaints is found in section 10.5. of the Privacy Policy, and merely refers to the possibility of lodging complaints through the state's legal systems at the Ministry of Transport and Communications, if users believe "processing" of their information "infringes applicable law." Although it does not specify which laws, data protection in Qatar is regulated by Law 13/2016 (Data Protection Law). The law stipulates the right for users not to have data processed for non-lawful purposes without their permission, the right to be informed of the purpose of the data being processed, and the right to have access to their data. However, as the only outlined way to lodge complaints is through the state (Ministry of Transport and Communications), and as the SC is a state entity, a conflict of interest could arise.

Additionally, the Hayya App and Portal and other SC platforms engage in practices that go beyond the limited scope of Qatari legislation such as targeted advertising and "profiling." As a result, users whose rights to privacy may be negatively affected by such practices would not have adequate access to remedy. The Privacy Policy states, however, that fans can complain to the Information Commissioner's Office in the UK and EU data protection authorities, if they are based in a country where privacy protections are robust.

To make use of this grievance mechanism and submit their complaints, users need to contact the SC via email addresses supposedly listed in section 12 of the privacy Policy. However, these email addresses are hidden from users, and those who click on them are redirected to a page that asks them to enable Javascript in order to decode the email addresses.



Screenshot of page that appears after clicking on email addresses provided by the SC in section 12 of its Privacy Policy.

Article 11 of the Data Protection Law requires data controllers to publish a policy for receiving data requests, such as complaints, access, corrections, and deletion requests. While the SC does outline a way to lodge complaints, it does not meet RDR standards of clear and predictable grievance and remedy mechanisms to address users' privacy concerns.[41] It also does not disclose evidence of providing remedy for users' privacy grievances such as apologies, restitution, financial or non-financial compensation, and guarantees of non-repetition of harm.

Law No.13 of 2016 Personal Data Privacy Protection, https://compliance.qcert.org/sites/default/-files/li-brary/2020-11/Law%20No.%20%2813%29%20of%202016%20%20on%20Protecting%20Personal%20Data%20Privacy%20-%20English.pdf.

No notification of changes to privacy policies

The privacy policies of the Hayya App and Portal have several shortcomings when it comes to expected standards for accessibility and disclosure of changes made to the privacy policies.

We expect companies to offer privacy policies that are easy to find and easy to understand. The Supreme Committee for Delivery and Legacy only partly meets these standards. When accessing the platform from a computer, the Privacy Policy is easy to find, through a link located at the bottom of the homepage together with the Cookie Notice. The policies are presented in a relatively understandable manner: both policy documents are visually clear and the language used is not overly complicated.

Indicator 2: Access to privacy policies

The SC should offer privacy policies that are easy to find and easy to understand.

Elements:

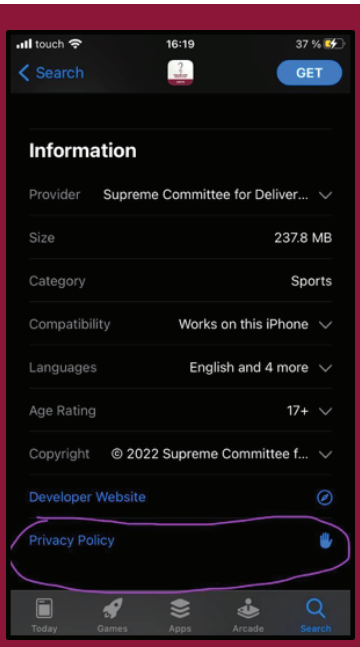
1. Are the SC's privacy policies easy to find?

2. Are the privacy policies available in the primary language(s) spoken by users in the company's jurisdiction?

3. Are the policies presented in an understandable manner?

However, they do have serious flaws and do not meet all the expected standards. First of all, both the Privacy Policy and the Cookie Notice are not available in both primary languages spoken in Qatar: available in English, but not in Arabic. As this is an international event with football fans from all around the world coming to Qatar, the Hayya Portal is available in German, Spanish, and French (in addition to Arabic and English). However, the policies are not available in these languages.

Another flaw with regards to accessibility is that accessing the Privacy Policy from Apple's App Store appears impossible. This is concerning, as users who will download the Hayya App on their iPhones do not have access to the Privacy Policy. For Android users, they are able to easily access the Privacy Policy via the app's page on Google Play.



Screenshot of the error page iPhone users are directed to when they click on the Privacy Policy from the app's page on App Store.

There is no way to access the policy from the app's homepage either.

Furthermore, we expect Hayya Portal and App to clearly disclose that they directly notify users about changes to the privacy policies, prior to these changes coming into effect.

Indicator 3: Changes to Privacy Policies

The SC should clearly disclose that it directly notifies users when it changes its privacy policies, prior to these changes coming into effect.

Elements:

1. Does the SC clearly disclose that it directly notifies users about all changes to its privacy policies?

2. Does the SC clearly disclose how it will directly notify users of changes?

3. Does the SC clearly disclose the timeframe within which it directly notifies users of changes prior to these changes coming into effect?

4. Does the SC maintain a public archive or change log?

The SC does not meet these standards, as it does not disclose that it directly notifies users about changes to its Privacy Policy or Cookie Notice. In the Privacy Policy, it discloses that changes will be posted on the platforms and are "available if you contact us," and that if the "changes are material, we will indicate this clearly on our Platform(s)." With regards to the Cookie Notice, it merely states that "we will inform you of any changes to this Cookie Notice by posting them on this page and updating the Cookie Table above." Both the Privacy Policy and Cookie Notice indicate that the SC will, in the case of changes made to their policies, update the date they were last changed. However, only the Cookie Notice has such a date indicated. Lastly, the company does not disclose a timeframe within which they notify users of changes, and there were no findings of the SC maintaining a public archive or change log.

User information handled with opacity

As a general overview, the Supreme Committee for Delivery and Legacy lacks transparency about its collection, inference, sharing and retention of Hayya users' information, falling short of RDR standards. It is transparent about which user information it collects and how, but does not list all the types of user information it infers and shares, nor its purposes for doing so. Its policy of user information retention falls short of RDR standards and it is unclear for how long information of Hayya App and Portal users is retained. Finally, users lack control over their user information and are able to only access it under "certain conditions."

The SC collects, infers, and shares information but fails to specify purposes

Indicator 4: Collection of user information

The SC should clearly disclose what user information it collects and how.

Elements:

1. Does the SC clearly disclose what types of user information it collects?

2. For each type of user information the SC collects, does it clearly disclose how it collects that user information?

3. Does the SC clearly disclose what user information it collects from third parties through non-technical means (i.e purchases, data-sharing agreements, and other contractual relationships with third parties)?

4. Does the SC clearly disclose that it limits collection of user information to what is directly relevant and necessary to accomplish the purpose of its service?

First, it clearly discloses what information Hayya collects and how this information is collected, with mentions of specific categories of user information and even examples. Additional details on collection of user information by SC are provided in Annexes B (Accommodation Portal), C (Hayya App), D (Hayya Card), E (Hayya Portal), and F (Qatar 2022 site) of the Privacy Policy.

For the Hayya App, Portal, and Card, which are the focus of our analysis, the lists of user information collected are comprehensive. Basic information such as name, date of birth, address, email address, telephone or mobile number is collected when fans register to use the Hayya application or apply for a Hayya Card via the Portal. The Hayya App collects location information if users enable tracking on their mobile devices, while the Hayya Card collects times and location of check-ins at stadiums.

Sensitive information is also collected. This includes health information on whether users applying for the card via the portal have symptoms of infectious disease, "particularly where there is an ongoing epidemic or pandemic." Users with disabilities may have information about their disability status collected if they submit "requests for disability access" at stadiums via the app.

While the SC is clear about the user information it collects and how, it does not mention which user information is collected from third parties through non-technical means, such as through purchases, data-sharing agreements, and other contractual relationships with third parties. It puts the onus on users to find out which information this is: "We may also receive information about you from third parties who are legally entitled to disclose that information. If you wish to know more about how these third parties handle your personal information, please contact them directly."

The entity does not commit to the principle of data minimization, but pledges not to collect minors' user information without legal guardian's consent.

When it comes to its practices of user information inference, the SC is even less transparent. Data inference involves the deployment of "big data" analytics and algorithmic decision making technologies to draw inferences and predictions about the behaviors, preferences, and private lives of its users. These methods might be used to make inferences about user preferences or attributes (e.g., race, gender, sexual orientation), and opinions (e.g., political stances), or to predict behaviors (e.g., to serve advertisements). Without sufficient transparency and user control over data inference, privacy-invasive and non-verifiable inferences cannot be predicted, understood, or refuted by users.[42]

In its Privacy Policy, the SC makes implicit references that it may be engaging in practices to infer user information. Under the section "Profiling and automated decision making" it mentions that it analyzes personal information, including preferences, how users interact with its platforms and previous ad clicks to show them "advertisements and recommendations."
It is also implied that user "preferences'' and "interests" are inferred, however, this is not clearly stated, and it is unclear which other user information may be inferred. In section 3.3 It is also implied that user "preferences'' and "interests"

Indicator 5: Inference of user information

The SC should clearly disclose what user information it infers and how.

Elements:

1. Does the SC clearly disclose all the types of user information it infers on the basis of collected user information?

2. For each type of user information the SC infers, does it clearly disclose how it infers that user information?

3. Does the SC clearly disclose that it limits inference of user information to what is directly relevant and necessary to accomplish the purpose of its service?

4. For each type of user information the SC collects, does the it clearly disclose its purpose for collection?

42 RDR methodology.

are inferred, however, this is not clearly stated, and it is unclear which other user information may be inferred. In section 3.3 of the Privacy Policy, the Committee states that it collects user information to "analyse your personal information and use of our Platforms in order to better understand your and other Fans' preferences and requirements, so as to better develop and organise our products, services and events." In the "Targeting / advertising cookies'' section of the Cookie Notice, it states: "These Cookies record information about your visit to our Platforms to help target advertising and to build a profile of you. For example, the pages you have visited, the links you have followed, the number of times you've seen an ad, the ads you have clicked on and your browsing habits / interests."

Finally, the policy does not mention any limits to inference of user information. On a jurisdictional level, there is no general requirement for consent prior to processing data in the Qatari Protection Law. The only requirement is that the data controller obtains consent if the processing is not for a legitimate purpose or for a purpose other than the purpose for which the data was processed.

When it comes to the sharing of user information, the SC specifies only one type of user information it may share: payment details. The SC states in section 4 of the Privacy Policy that it shares such information with banks and payment service providers when users make payments using the Hayya App or Card. It does not specify what other types of information it may share and with which parties, nor does it disclose the names of all the third parties with which it shares user information.

Indicator 6: Sharing of user information

The SC should clearly disclose what user information it shares and with whom.

Elements:

1. For each type of user information the SC collects, does it clearly disclose whether it shares that user information?

2. For each type of user information the SC shares, does it clearly disclose the types of third parties with which it shares that user information?

3. Does the SC clearly disclose that it may share user information with government(s) or legal authorities?

4. For each type of user information the SC shares, does it clearly disclose the names of all third parties with which it shares user information?

It does, however, state that it may disclose user information with governmental agencies, including the Ministry of Public Health, the Ministry of Interior, and the Ministry of Transport and Communications, "so that they may carry out any checks required to ensure the safety and security of the Tournaments." User information may also be shared with law enforcement authorities inside or outside Qatar "to comply with any legal obligation."

The SC is not transparent about its purposes for collecting, inferring, and sharing information of users of its Hayya App and Portal. It provides general use purposes such as to "communicate effectively with you and conduct our operations," "provide you with marketing materials," and "ensure the safety and security of our operations, premises and events," among other purposes listed in section 3 of the Privacy Policy.

However, it does not break down these purposes per each type of user information collected nor does it specify the user information it collects through non-technical means and its purposes for doing so. It does, however, make implicit references that it may be engaging in practices to infer user information, specifically "preferences'' and "interests" to "understand" users and for targeted advertising purposes in section 4.

Indicator 7: Purpose for collecting, inferring, and sharing user information

The SC should clearly disclose why it collects, infers, and shares user information.

Elements:

1. For each type of user information the company collects, does it clearly disclose its purpose for collection?

2. Does the SC clearly disclose its purpose for collecting user information from third parties through non-technical means (i.e purchases, data-sharing agreements, and other contractual relationships with third parties)?

3. For each type of user information the company infers, does it clearly disclose its purpose for the inference?

4. Does the SC clearly disclose whether it combines user information from various company services and if so, why?

5. For each type of user information the company shares, does it clearly disclose its purpose for sharing?

6. Does the SC clearly disclose that it limits its use of user information to the purpose for which it was collected or inferred?

In section 3, it does imply that it shares payment information with banks and payment service providers to process payments of Hayya Card and App users. These are the only two cases where purposes could be tied with specific types of user information shared or inferred.

In fact, as explained above, the SC fails to even specify each type of user information it infers or shares. Finally, there is no clear indication whether or not the SC combines user information from various company services, and there is no commitment from its part to the principle of use limitation (i.e. user information should not be used for purposes beyond those for which it was collected or inferred).

User information retained "for as long as is necessary"

The SC's user information retention policy is vague, which makes it impossible for Hayya users to know for how long their information is retained. No specific retention periods are provided, and the Privacy Policy vaguely states that user information is retained "for as long as is necessary for the processing purpose(s) for which the information was collected, and any other permissible, related purpose."

There is no commitment from the SC that it will delete all user information after users terminate their Hayya accounts and within which timeframe. But, it is vaguely stated that if user information is no longer needed it will either be "irreversibly" anonymized or "securely" destroyed, without specifying what de-identified user information will be retained in this case and the process for de-identifying it. This is generally considered to not be best practice as to truly anonymize data is extremely difficult and thus this caveat leaves the SC with the potential to keep data it does not need for longer periods of time or indefinitely.

Indicator 8: Retention of user information

The SC should clearly disclose how long it retains user information.

Elements:

1. For each type of user information the company collects, does the SC clearly disclose how long it retains that user information?

2. Does the SC clearly disclose how long it retains the user information it collects from third parties through non-technical means?

3. Does the SC clearly disclose what de-identified user information it retains?

4. Does the SC clearly disclose the process for de-identifying user information?

5. Does the SC clearly disclose that it deletes all user information after users terminate their account?

6. Does the SC clearly disclose the time frame in which it will delete user information after users terminate their account?

The Qatari data protection law does not set specific retention periods, but only states in Article 10 that "the Controller shall not keep any Personal Data for a period of time that exceeds the necessary period for achieving such purposes."

Finally, Hayya users lack options to control and access their own information. In its Privacy Policy, the SC only mentions a vague and general "withdrawal" right and an option for users to limit collection of their location information via their device settings. It does not disclose options for users to control collection of their information for each type of user information it collects.

In the "Your rights" section, the SC discloses the following: "Where processing of your personal information is based on your consent, you have the right to withdraw it at any time. Please note that the withdrawal of your consent will not affect the lawfulness of processing based on your consent as carried out before such withdrawal." In Annex C, it mentions that location data in the app is collected if users enable tracking. This type of information may be used "for crowd control and tournament management purposes," and one can assume that users have control over this information through their devices since they need to enable tracking for their location information to be collected in the first place.

However, it is not specified which other user information can be controlled by users by withdrawing their consent or by any other options. Users' ability to delete their information is limited to that which the SC "no longer have a lawful ground to use," and it is not specified which types of user information are these. Options for users to control attempts to infer their user information and delete inferred data are not provided.

Indicator 9: Users' control over their own user information

The SC should clearly disclose to users what options they have to control the company's collection, inference, retention and use of their user information.

Elements:

1. For each type of user information the SC collects, does it clearly disclose whether users can control the company's collection of this user information?

2. For each type of user information the SC collects, does it clearly disclose whether users can delete this user information?

3. For each type of user information the SC infers on the basis of collected information, does it clearly disclose whether users can control if it can attempt to infer this user information?

4. For each type of user information the SC infers on the basis of collected information, does it clearly disclose whether users can delete this user information?

When it comes to users' access to their own user information, Hayya App and Portal users may have the right to "be provided with a copy of information [they] provided to the SC," under "certain conditions." The conditions are not clear. In Section 10.5 of the Privacy Policy, the SC states that users' exercise of their access rights, among other rights, "is subject to certain exemptions to safeguard the public interest (e.g. the prevention or detection of crime) and our interests (e.g., the maintenance of legal privilege)."

Indicator 10: Users' access to their own user information

The SC should allow users to obtain all of their user information it holds.

Elements:

1. Does the SC clearly disclose that users can obtain a copy of their user information?

2. Does the SC clearly disclose what user information users can obtain?

3. Does the SC clearly disclose that users can obtain their user information in a structured data format (i.e., an easily manipulable format such as a CSV file)?

4. Does the SC clearly disclose that users can obtain all public-facing and private user information it holds about them?

5. Does the SC clearly disclose that users can obtain all the information that it has inferred about them?

The SC does not clarify what user information users can obtain and whether or not users can obtain their information in a structured data format.
The policy allows users to ask the SC to "transmit" to them the personal information they provided but there is no clear disclosure that users can obtain all of their information. No disclosures were found on whether users can obtain all the information that a company has inferred about them either.

From a legal perspective, Qatar's data protection law prescribes certain control, access and erasure rights. As mentioned previously, article 4 stipulates that a controller can only process personal data with consent of the user, "unless data processing is necessary to achieve a Lawful Purpose for the Controller or other recipient of such data."

Pertaining to control over personal data, article 5 states that an individual: may "withdraw the prior consent thereof for Personal Data Processing"; may under certain circumstances object to processing of Personal Data; and may request corrections to, and, under certain circumstances, the "omission or erasure" of their data. While it stipulates the users' right to object to processing, the article does not disclose procedures for responding to such requests.

Article 7, however, stipulates that "the controls and procedures, related to individuals' exercise of rights provided for in the two preceding Articles, shall be specified by a decision of the Minister." Falling under this provision, are the rights stipulated in Article 6: for individuals to, "at any time, access the Personal Data thereof and apply to review the same"; and the right to "obtain a copy of the Personal Data thereof after paying an amount that shall not exceed the service charge."

Users are tracked and their information is monetized, yet they lack control over targeted advertising

The SC engages in targeted advertising and tracking across its platforms. In Section 3 of the Cookie Notice, it states that it racks users' browsing habits to help it understand how their platforms, including the Hayya App and Portal, are used so they "can improve them and generate more revenue" and deliver ads that are "more relevant" to the "interests" of its users. Yet, the Committee provides only limited information regarding these practices and how users can control them.

Indicator 11: Advertising targeting rules and enforcement

The SC should clearly disclose its policies governing what type of advertising targeting is prohibited.

Elements:

1. Does the SC clearly disclose whether it enables third parties to target its users with advertising content?

2. Does the SC clearly disclose what types of targeting parameters are not permitted?

3. Does the SC clearly disclose that it does not permit advertisers to target specific individuals?

4. Does the SC clearly disclose that algorithmically generated advertising audience categories are evaluated by human reviewers before they can be used?

5. Does the SC clearly disclose information about the processes and technologies it uses to identify advertising content or accounts that violate the company's rules?

It is unclear what the SC's advertising targeting rules are and how they are enforced. It clearly discloses in its Cookie Notice that it allows its advertising partners to target users with advertising by using cookies to track them, record their information, and build a profile of them. The targeting parameters set out by the SC include users' browsing habits and interests. The language used is not comprehensive and there is no mention of prohibited targeting parameters.

The SC also permits advertisers to engage in the problematic practice of targeting specific individuals via their email addresses. Its processes of identifying advertisers who violate this policy is not set out. The Privacy Policy includes a section on automated decision making for profiling and advertising but the information provided is vague, and it is unclear if advertising audience categories generated using algorithms are evaluated by human reviewers before they are deployed. Advertising audience categories are groups of users, identified for the purpose of delivering targeted advertising, who share certain characteristics and/or interests, as determined on the basis of user information that a company has either collected or inferred. Ensuring human review of algorithmically-generated categories is designed to address the problematic practice of allowing categories created by machine learning to move directly into an ad-targeting interface, which could lead to categories such as people with racial animosity or people who are emotionally vulnerable to certain advertising appeals.

The SC provides general information about its collection of third-party information through technical means. It discloses some information it collects using cookies. In the Cookie Notice, it hints that it uses cookies to track users' interactions with ads on its platforms and other websites: "Cookies can also help ensure that any adverts that you see on our Platforms and other websites are more relevant to you and your interests."

It also states that it collects statistical information to understand how users interact with the SC's social media presence using social media platforms' "non-essential tracking technology." It is unclear what other user information may be collected from third-parties through technical means and for what purposes.

Indicator 12: Third-party tracking
The SC should clearly disclose its practices with regard to user information it collects from third-party websites or apps through technical means.

Elements:

1. Does the SC clearly disclose what user information it collects from third-party websites or apps through technical means?

2. Does the SC clearly explain how it collects user information from third parties through technical means?

3. Does the SC clearly disclose its purpose for collecting user information from third parties through technical means?

4. Does the SC clearly disclose how long it retains the user information it collects from third parties through technical means (such as cookies and widgets)?

5. Does the SC clearly disclose that it respects user-generated signals to opt out of data collection?

The SC does not specify retention periods for this information. Its Privacy Policy merely states information will be retained "for as long as is necessary for the processing purpose(s) for which the information was collected, and any other permissible, related purpose."

Users' control over targeted advertising and tracking is relegated to actions users can do in general to control cookie tracking. The Cookie Notice explains how first party and third-party cookies work and provides information on how users can stop cross-site tracking through their browser settings and how they can block third-party cookies by installing cookie blocking mechanisms.

Although information is provided on how to block cookies, the SC does not explicitly state that its platforms respect user-generated signals not to be tracked. One way users can send such signals is through the Do Not Track feature, which allows users to request websites not to track them. However, such requests are not always respected by web services and platforms.

44 RDR methodology.

Information about targeted advertising opt-out/opt-in options is limited to "marketing" operations via direct contact and "in-app marketing" and does not include the opt-out options for the Hayya Portal. In section 5 of the Privacy Policy, the SC uses the term "marketing" but it is clear these operations fall under "targeted advertising." In fact, it mentions that it may, along with "selected third parties or affiliates" use "your data...to provide you with information about goods and services which may be of interest to you and we or they may contact you about these by post, email, SMS, phone, in-app marketing or through social media channels."

Indicator 13: Control over targeted advertising

The SC should clearly disclose options for users to control the use of their information for targeted advertising.

Elements:

1. Element 1: Does the SC clearly disclose that it provides users with options to control how their user information is used for targeted advertising?

2. Element 2: Does the SC clearly disclose that targeted advertising is off by default?

3. Element 3: Does the SC clearly disclose that users can access the list of advertising audience categories to which the company has assigned them?

Targeted advertising is off by default in some cases. The SC sets out that it will ask for consent where required by law, which implies that targeted advertising is on by default in places where the law does not require users' prior consent. It is also unclear if when signing up, the box to receive marketing is already ticked and that users would have to be vigilant in unticking the box. This form of consent is prohibited under more robust regulatory frameworks, such as the EU's Global Data Protection Regulation (GDPR), as opt-out systems cannot be considered true consent. The policy does not grant users access to the advertising audience categories that have been assigned to them.

Qatari law overwhelmingly does not regulate targeted advertising or tracking, therefore the SC position is not in contravention of regulations. There is no regulation requiring users to have control over how their data is being used, disclosure of advertising targeting policies, or use of algorithmic systems to track, profile users, and target them with advertising. According to article 4 of the Qatar Data Protection Law, data controllers must obtain consent if the processing is not for a legitimate purpose or for a purpose other than the purpose for which the data was "processed." Thus, targeted advertising is not legally required to be off by default, except in specific scenarios where consent is needed, however there is no explicit information on what qualifies as consent. There are also no laws preventing the SC from being transparent about its targeted advertising policies and practices.

Overall the Hayya App and Portal do not provide enough information to users as the SC lacks transparency. Rather than designing a policy that respects privacy from the outset, it requires users to actively engage in privacy-protecting measures that are only effective for some of the targeted advertising and tracking processes.

Vague process for handling government surveillance demands

Information surrounding surveillance is scarcely provided by the SC. The Committee does not clearly state its process for responding to government demands for user information but mostly offers vague statements that it may disclose information to comply with legal obligations.

Under section 3.7 of the Privacy Policy, it discloses that "this may include disclosing your personal data to third parties, the court service and/or regulators or law enforcement agencies in connection with enquiries, proceedings or investigations by such parties anywhere in the world or where compelled to do so."

The SC further states in section 4.1.3 of the same policy that it may share personal information with government agencies, including the Ministry of Public Health, Ministry of Interior, and the Ministry of Transport and Communications to perform any safety and security checks for the tournament. There is no differentiation within the policy regarding how the Committee will respond to the demands of different government agencies such as court orders or non-judicial demands.

It is also unclear how the SC handles demands from foreign jurisdictions, stating merely in section 4.2 of the Privacy Policy that in "exceptional circumstances," it may share user information "in order to comply with any legal obligation" inside or outside Qatar. The SC does not commit to carry out due diligence on these demands before responding, nor does it commit to push back on inappropriate or overboard demands.

Indicator 14: Process for responding to government demands for user information

The SC should clearly disclose its process for responding to governments demands for user information.

Elements:

1. Does the SC clearly disclose its process for responding to non-judicial government demands?

2. Does the SC clearly disclose its process for responding to court orders?

3. Does the SC clearly disclose its process for responding to government demands from foreign jurisdictions?

4. Do the SC's explanations clearly disclose the legal basis under which it may comply with government demands?

5. Does the SC clearly disclose that it carries out due diligence on government demands before deciding how to respond?

6. Does the SC commit to push back on inappropriate (do not come from the appropriate authority or follow the proper legal process), or overbroad government demands?

7. Does the sc provide clear guidance or examples of implementation of its process for government demands?

With so little information given, it is not possible for fans attending the 2022 World Cup to understand how the SC may respond to government demands asking for their information.

No data is provided regarding the number of government demands for user data, foreign or domestic. The SC's compliance rates and the number of fans affected by these government surveillance demands is thus unclear. It is also not clear if the SC plans to publish such data at a later stage. However, given the general regulatory environment in Qatar which does not encourage transparency in these areas and fails to sufficiently protect privacy, such disclosure remains unlikely.

Indicator 15: Data about government demands for user information

The SC should publish data about government demands for user information.

Elements:

1. Does the SC list the number of government demands it receives by country?

2. Does the SC list the number of accounts affected?

3. Does the SC identify the specific legal authority or type of legal process through which law enforcement and national security demands are made?

4. Does the SC include government demands that come from court orders?

5. Does the SC list the number of government demands it complied with, broken down by category of demand?

6. Does the SC list what types of government demands it is prohibited by law from disclosing?

Under Qatari law, there is no requirement on the companies and entities to disclose information, such as the number of user information demands or the process of responding to them, but equally there is no law preventing such transparency disclosures either.

Government surveillance in Qatar in general is not extensively regulated. Article 37 of the Qatari constitution[46] enshrines the right to privacy, but other legislation that could enforce this right has many broad exemptions. Under the data protection law, there are significant exemptions whereby "the competent authority may decide to process some personal information" without consent or need to inform users if it is in the interests of "protecting national and public security, protecting international relations of the state, protecting the economic or financial interests of the state, and preventing any criminal offense or gathering information thereon or investigating therein."

Government surveillance is mostly regulated by the 2006 Telecommunications Law, which states in Chapter 15 that the Secretariat-General of Telecommunications and Information Technology "request the Service Providers or others to supply information necessary for the exercise of its powers," and that the information shall be furnished in the form, manner and time as the government specifies. [47]

46 "Qatar's Constitution of 2003," Constitute Project, https://www.constituteproject.org/constitution/Qatar_2003.pdf?lang=en.

47 Qatar Telecommunications Law, Chapter 15, Article 62.

Security policies and measures: a blindspot

The SC lacks transparency about security policies and measures in place to protect information of users of the Hayya App and the Hayya Portal.

There is no disclosure regarding measures to limit and monitor employee access to user information; no indication of a security team conducting audits on the company's products and services; and no indication that it commissions third parties to conduct such audits.

Indicator 16: Security oversight
The SC should clearly disclose information about its institutional processes to ensure the security of its products and services.

Elements:

1. Does the SC clearly disclose that it has systems in place to limit and monitor employee access to user information?

2. Does the SC clearly disclose that it has a security team that conducts security audits on the company's products and services?

3. Does the SC clearly disclose that it commissions third-party security audits on its products and services?

In Article 2 of the Terms of Use, the SC specifies that it takes reasonable (unspecified) precautions to prevent the presence of viruses and malwares on the website. However, rather than informing users and the public about any of its measures, the SC seems more concerned with safeguarding itself against any liability. In section 2.1 of the Terms of Use, it states that it will not accept any responsibility over "direct, indirect, incidental, special or consequential damages" deriving from the use of its products. These damages include "damages for loss of profits, goodwill, use, data or other intangible losses" happening as a result, among others of "unauthorised access to the website" or "any other matter relating to the website." Under Qatar's Personal Data Privacy Protection, data controllers are required to take "appropriate administrative, technical and financial precautions" to protect user information.

The SC provides no mechanism through which security researchers can report vulnerabilities; equally, there is no indication of a timeframe in which the company will review reports of vulnerabilities or commitment to not pursue legal actions against these researchers. It is only stated in section 3.3 of the Terms of Use that users "shall immediately notify SC" if they learn of "suspect or unauthorized use" of their accounts or breaches to the terms "or any other breach of security."

Indicator 17: Security vulnerabilities
The SC should address security vulnerabilities when they are discovered.

Elements:

1. Does the SC clearly disclose that it has a mechanism through which security researchers can submit vulnerabilities they discover?

2. Does the SC clearly disclose the timeframe in which it will review reports of vulnerabilities?

3. Does the SC commit not to pursue legal action against researchers who report vulnerabilities within the terms of the company's reporting mechanism?

The SC's process of dealing with data breaches that may occur on the Hayya App and Portal is equally unknown: no information is given for this process, including notification of relevant authorities, process for the notification of the affected data subjects or the addressing of the impact of the breach. Article 14 of the Qatari Data Protection Law does require a data controller to notify both the government and the user "if such breach may cause serious damage to Personal Data or individual privacy."

The Committee does not disclose anything either about encryption methods it uses.

Finally, with regards to account security, the SC does not disclose use of advanced authentication to prevent fraudulent access such as two-factor authentication (2FA) or multi-factor authentication. These methods require the user to provide separate pieces of evidence in combination to access their account—for example, requiring a login password plus a code delivered via a separate email account or text message, an authenticator app, a security token, etc. No mechanisms through which users of the Hayya App and Hayya Portal can view their recent account activity were provided by the SC, which also failed to provide a commitment to notify users in case of unusual activity and possible unauthorized access to their accounts.

Indicator 18: Data breaches
The SC should publicly disclose information about its processes for responding to data breaches.

Elements:

1. Does the SC clearly disclose that it will notify the relevant authorities without undue delay when a data breach occurs?

2. Does the SC clearly disclose its process for notifying data subjects who might be affected by a data breach?

3. Does the SC clearly disclose what kinds of steps it will take to address the impact of a data breach on its users?

Indicator 20: Encryption
The SC should encrypt user communication so users can control who has access to it.

Elements:

1. Does the SC clearly disclose that the transmission of user communications is encrypted by default?

2. Does the SCclearly disclose that transmissions of user communications are encrypted using unique keys?

Indicator 21: Account security
The SC should help users keep their accounts secure.

Elements:

1. Does the SC clearly disclose that it deploys advanced authentication methods to prevent fraudulent access?

2. Does the SC clearly disclose that users can view their recent account activity?

3. Does the SC clearly disclose that it notifies users about unusual account activity and possible unauthorized access to their accounts?

Recommendations

Based on the above findings, we have the following recommendations for the SC:

- **Strengthen remedy and grievance mechanisms.** The SC should provide Hayya users with robust grievance and remedy mechanisms that cover all the range of possible harms that may affect spectators while using the portal or the application.

- **Clarify handling of user information.** The SC should specify the user information it infers and shares, and its purposes for collection, inference, and sharing. It should limit collection of user information to what is directly relevant and necessary to accomplish the purpose of its service and use user information only for the purposes for which it was collected or inferred. It should also specify for how long it retains user information and commit to deleting all user information after users terminate their accounts.

- **Put users in control of their information.** The SC should provide users with clear options to control collection and inference of their information and delete all the types of information collected or inferred about them. Hayya users should also be able to access and obtain all the user information the SC has collected or inferred about them. Finally, the SC should prohibit advertisers from targeting specific individuals using their email addresses or any other specific identifiers. It should clarify that targeted advertising is off by default in all cases, not just "where required by law," and respect user generated signals not to be tracked.

- **Be transparent about handling government surveillance demands.** The SC should clarify how it responds to government demands —domestic and foreign— for user information. It should also disclose data about the number of these demands it receives, including compliance rates and the number of fans affected by them.

- **Put in place strong security policies.** The SC should disclose and implement robust policies and measures to protect the information of Hayya users. These should include mechanisms to limit and monitor employee access to user information, conducting internal and third-party security audits, and a clear policy for notifying the authorities and affected users of data breaches when they occur.