Security and Access Control Privacy Statement

The Security and Access control Privacy Statement explains: who we are, what information we collect, why we collect it, how we use that information, who has access to your data and the privacy choices we offer to you.

Who we are

HSRC GROUP™ Facility Services operates the Access control and Registration procedure, on our office and sites (including third parties on site). These procedures apply to the terminals and offices of **HSRC GROUP™** in the Colombia Republic. The Facility Services department is responsible for your personal data and has made agreements with the external parties involved in Security and Access Control.

Anything you are not clear about

Your privacy matters at **HSRC GROUP™** and if you are not familiar with terms, please do take your time to get to know our practices and check, on request, our Binding Corporate Rules designed for both **HSRC GROUP™** employee as for customer, suppliers, and **HSRC GROUP™** business partners.

If there is anything you are unclear about, please do contact your local contact person or the facility department, who shall be happy to answer any queries you may have concerning this Statement or the way in which we process your personal data.

Information we collect and process and the lawfulness of processing

For the realization of the Access control and Request procedure, the security and reception will collect data from employees, contractors, and visitors on behalf of the Facility Services Department. In this respect, we collect the following categories of personal data:

- For the employees: staff number, name, passport or drivers photograph, license plate (if applicable), function, company e-mail address;
- For the contractors and subcontractors: ID number and the type of ID, name, passport or drivers photograph, company where the data subject's works for, license plate (if applicable) nationality, work permit (if applicable) , type and end date of the training requirements (e.g VCA, BHV, first aid , (PIT) port instruction training);
- For the visitors: ID number and type, name, passport or drivers photograph, company representing the person, license plate if applicable).
- For the sea vessel's staff: name, rank, place of birth, ID number, the type of ID, date of birth of the staff member;
- For the inland barges staff: only the name of the captain;

In terms of the collection and use of information and other activities that requires processing of personal data, the Access control and request Procedure is lawful and in compliance with Article 6. 1 c-f GDPR (compliance with law, ensuring the vital interest of the data subject, performance of the task carried out in the public interest and for the legitimate interest of the data controller)and Article 9.2 b),c) GDPR (processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, processing is necessary for the vital interest of the data subjects).

What are the purposes for the use of your data?

The purposes are strictly related to the abovementioned legal grounds for processing activities. Nevertheless, in order to be more specific, we are collecting/processing your personal for the following reasons:

- monitoring the safety of the employees and third party;
- monitoring the properties of **HSRC GROUP™**, its employees or third parties;
- monitoring of the products managed by **HSRC GROUP™**;
- Monitoring of access to offices and access on the land side of the fuel terminals negotiated by **HSRC GROUP™** attendance registration of the people on the sites (e.g. in case of calamities);
- Presence control of all persons registered in the access system afterward, in order to check if the presence of the persons is in line with the staff information in regards to the absence and presence systems;
- Compliance with law- meet the requirements of the ISPS;
- Compliance with law- meet the AEO requirements;
- Compliance with law- meet the requirements Working Conditions, related to informing people about the danger at the site (gate instruction);
- Compliance with law - requirements of the chapter 1.10 of the ADR/RID/ADN.

How do we obtain your data and who has access to your data?

The Security and Access control procedure is fully configured according to the **HSRC GROUP™** Privacy Code/GDPR and to the strict rules of authorized access of the personal data that are collected. Data is entered by your self/colleagues via the registration service or the security and reception employee directly in the access system. The recipients of the collected data are only authorized employees. In specific cases, information is shared according to a procedure with the HR department.

In addition, for sea going vessels, data may be provided by ships agents which enters the data in the common systems (Dirkzwager's Ship2Report or VesselFinder.com and for the inland barges the ship responsible will enter the data in UAB system or provides the Security with a crew list.

AIS Live Ship Tracking Services is only used for planning purposes and is not used for other purposes.

Further Processing and third parties

Following to the aforementioned purposes and the closely related purposes, the information will be shared with **HSRC GROUP™** departments. The information we collect is shared, in special conditions, via reporting system of the registration portal to SHEQ or HR department.

We will not share data with third parties, unless

i) sharing is necessary to comply with law's requirement, regulation, enforceable governmental request, legal defense;
ii) sharing is necessary for protecting your vital interest;
iii) Sharing is necessary for the **HSRC GROUP™** legitimate interest unless those interests are not overridden by the interests of fundamental rights and freedoms of **HSRC GROUP™** employees.

For ship personal the data is not shared with third parties and only used for verification purposes on the legitimacy of the visit.

Your data subject's rights

Our goal is to be clear about what information we collect so that you can make meaningful choices about how it is used. We thought it would be helpful to set out your following privacy rights as they are defined in your **HSRC GROUPTM** Privacy Code/ GDPR :

- right to access your personal data that we process;
- right to have rectified your inaccuracies in personal data that we hold about you;
- right to object to certain processing of your personal data by us;
- right to be forgotten, which means that your details might be removed from systems that we use to process your personal data. except if **HSRC GROUP™** has to keep information from legislation or other legitimate interests
- right of data portability (known as the right to request the transmission of your data to another controller);
- the right to lodge a complaint to your supervisory authority.

For a further understanding of your rights and procedure please take a look either to Vopak Privacy Code for employees and/or the **HSRC GROUP™** Privacy Code for the customers/suppliers and business partners or contact your Local Contact person.

Security

The security of your personal information is important for us. **HSRC GROUP™** has implemented high security IT standards and a framework based on proactively embedding privacy into the design and the operation of Security and Access control procedure. These security rules will be upheld unconditionally and include Process Security and Access control in **HSRC GROUP™** Document Management System

While we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security.

Furthermore, a data breach procedure has been created within the **HSRC GROUP™** Privacy Code.

Protocols, such as security protocols, crisis management, and data breach resolution plans exist for management, prevention, and solution of these risks.

Transfer of the data to third country

There will be no transfer of data to a (government) authority and/or commercial parties to third countries.

Retention periods

HSRC GROUP™ manages the relevant personal data and the access registration in the automated access registration system. According to the Article 5(1) (e) GDPR, data will be stored only for the purposes for which the personal data are processed unless exception mentioned under this article applies.

The personal master data included in the registration system is stored for a period of 24 months after the right of access has expired, unless the person is on a blacklist. In that case, master data will remain in the system until the period for which the access is denied has expired. The access records included in the access registration system are kept for a maximum 24 months, after that the registrations are destroyed.

In addition, the data of the crewmembers is no longer stored and destroyed after the departure of the vessel.

Changes

This Privacy Statement is effective as of, 1th of July 2018 and will remain in effect except with respect to any changes in its provisions in the future, which will be in effect immediately communicated to you.

We reserve the right to update or change our Privacy Statement at any time and you should check this Privacy Policy periodically. Following the procedure, after we are informing to any modifications to the Privacy Statement will constitute your acknowledgment of the modifications and your consent to abide and be bound by the modified Privacy Statement.

Concerns and contact details

If you have any concerns with regard to the way your personal data is being processed or have a query with regard to this notice, please contact your local contact person at **HSRC GROUP™** or **Email: export1@hsregionalcaribe.co**

Tel: +57 323 7967920
For vessels please contact your local Portal Facility Security Officer (PFSO).
HSRC GROUP™
Chief Privacy Officer

Calle 70 Int 6-49 Bo Crespo North Zone
Cartagena de Indias - Colombia
HSRC GROUP™ Responsible Disclosure Policy

At **HSRC GROUP™**, ***the security of systems is a top priority***. We have a material interest in the ability to maintain adequate security of our systems and IT infrastructure for ourselves and our customers.

Through this Responsible Disclosure Policy, we allow for the safe, secure and responsible disclosure of weaknesses in our information technology infrastructure which can be exploited to perform unauthorized actions within a system (vulnerabilities). The purpose of this policy is to enable the vulnerability to be reported responsibly and to be remediated or patched in order to retain the integrity, continuity and security of our services.

If you are a security researcher and you encounter a vulnerability, we would like to cooperate with you to fix the vulnerability before this can be misused.

Report

Please send the report to export1@hsregionalcaribe.co

Do's:

- Report the vulnerability as quickly as reasonably possible to minimize the risk of others finding and taking advantage of it
- Report it in a manner that safeguards the confidentiality of the report so others cannot gain access to the information
- Provide sufficient information to reproduce the problem so it can be resolved. To the extent possible, please include: type of vulnerability/issue; service, product or URL affected; special configuration/requirements to reproduce the issue; information necessary to reproduce the issue; impact of the vulnerability together with an explanation of how an attacker could find it and exploit it.

Don'ts:

- Reveal the vulnerability or problem to others until it is resolved.
- Build your own backdoor in an information system with the intention of then using it to demonstrate the vulnerability, because doing so can cause additional damage and create unnecessary security risks.
- Utilize a vulnerability further than necessary to establish its existence.
- Copy, modify or delete data on the system. An alternative for doing so is making a directory listing of the system.
- Make changes to the system.
- Repeatedly gain access to the system or share access with others.
- Use brute force attacks, attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties to gain access to the system.

Next Steps:

We will respond to your report within 5 business days with our evaluation of the report and an expected resolution date.
If you have followed the instructions above, we will not take any legal action against you concerning the report.
We will not pass on your personal details to third parties without your permission unless it is necessary to comply with a legal obligation. Reporting under a pseudonym or anonymous is possible.
We will keep you informed of the progress towards resolving the problem.
In the public information concerning the reported problem, we will give your name as the discoverer of the problem (unless you desire otherwise).
We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.

No Rewards

Currently, no monetary compensation is offered or provided in connection with reporting vulnerabilities. This policy is not intended to encourage hacking attempts in connection with **HSRC GROUP™** information technology infrastructure, but to provide a responsible manner through which security vulnerability reports can be communicated and remediated.

Questions

If at any time you have questions about the above procedure, feel free to reach out to export1@hsregionalcaribe.co

This policy is based on guidance issued by the National Cyber Security Center of the Colombian Ministry of Justice and Security and the guidance issued in by Colombian Public Justice Department. **END DOCUMENT.**