Notice of Data Security Incident

Dear Guest,

As we have previously communicated, Hurtigruten was affected by a data security incident in December 2020. We are providing this updated information on the data security incident that has affected some Hurtigruten guests' information.

Our investigations indicate that information for some guests having booked expedition voyages with MS Midnatsol for sailings in the period 2016 to 2020 and for MS Fram for sailings in the period from 2018 to 2020 have been affected by the incident.

We have notified all guests affected by the incident directly to the extent we have contact information to such guests. As we do not have contact information to all affected guests, this notice is placed as an attempt to reach the guests to whom we do not have contact information.

What happened?

On December 14, 2020, we learned that an unauthorized actor gained remote access to our network and encrypted parts of our computer systems. At that time, however, we were unable to determine which guests may have been affected, if any, and what information might have been accessed.

We immediately disabled affected computer systems, took down their internet connection to prevent any further intrusion and launched a forensic investigation to determine the nature and scope of the incident. We understand that Hurtigruten was one of many companies that was a victim of this type of intrusion.

On February 18, 2021, the unauthorized actor placed some of the above information on a difficult to access part of the internet.

What Information Was Involved?

Based on our investigations, we have recently determined that the affected information for the guests to whom we do not have contact information involves:

- Guest name, date of birth, nationality,
- For Midnatsol guests and some Fram guests, the information involves passport number and passport expiration date; and
- for some guests, the affected information also involves expired e-mail address, mailing address and phone number.

Hurtigruten **does not** store credit or debit card information.

What We Are Doing?

As noted above, we immediately took steps to contain the issue and commenced an investigation to determine the data and individuals that may have been affected.

We reported this matter to Norwegian law enforcement and the Norwegian Data Protection Authority (since Hurtigruten is based in Norway) and the Federal Bureau of Investigation. We also notified other applicable privacy regulatory authorities.

Over the past years we have made significant investments in data privacy and cyber security. Since this incident, we have further strengthened these efforts and our internal experts are working closely with third-party cybersecurity experts to further enhance the security of our systems and reduce the risk of a similar event happening in the future.

What Can You Do

We do not have any indication of actual harm to affected individuals as a result of this incident, but as we cannot completely rule out that someone may try to misuse your information, we still recommend you follow the enclosed additional steps that you can take to protect your personal information.

We sincerely regret any concerns or inconvenience that this incident may cause you.

For More Information

If you have questions or require further assistance, please contact us via one of these channels:

Website: https://www.hurtigruten.com.au/info/

Phone: +611800841599

Opening hours:

Monday to Friday	Saturday	Sunday
GMT+11 08:00-20:00	Closed	Closed

Sincerely,

HURTIGRUTEN

RECOMMENDED GUIDANCE FOR AFFECTED AUSTRALIAN CUSTOMERS

Hurtigruten has notified you of a recent data breach affecting personal information for a limited number of guests having booked expedition voyages with MS Midnatsol for sailings in the period 2016 to 2020 and for MS Fram for sailings in the period from 2018 to 2020.

We do not have any indication of actual harm to affected individuals as a result of this incident. However, we still recommend that you take the following steps to protect your personal information.

What can you do?

- Take steps to update your passwords for your online accounts immediately using strong passwords with a combination of letters (lower and upper caps), numbers and symbols and avoid storing sensitive or personal information on your email account.
- Make sure you are always cautious about responding to unsolicited emails or text messages and avoid clicking on any links contained within an email or text message unless the sender can be verified.
- Be particularly cautious of any phishing emails. These are emails that look like legitimate emails but are actually sent by fraudulent third parties posing as legitimate individuals or companies in an attempt to get you to disclose personal information, including identification and payment details. In particular you will not receive any emails or messages form Hurtigruten asking you to provide your personal information.
- The Australian Passport Office can assist you in applying for a new passport if you are concerned that you could be a victim of passport fraud. We recommend contacting the Australian Passport Office to voice your concerns prior to commencing this step and seek any further guidance from them in relation to protecting your passport details. Their contact details are: passports.fraud@dfat.gov.au or by phone on 131 232.

Your privacy rights

For more information about how we collect and handle your personal information and how to exercise your privacy rights in relation to the personal information we hold about you, please refer to our privacy policy available online at https://www.hurtigruten.com.au/practical-information/statement-of-privacy/ or by calling us at +611800841599.

For more information about your privacy rights under Australian law, how you can protect your privacy information and how to make a complaint, please visit the OAIC website at https://www.oaic.gov.au/ or contact the OAIC at 1300 363 992.