Dear Picasso Customer,

On June 9th at 02.53, Techotel and our customers were subjected to a comprehensive high-tech hacker attack, in which criminals gained unauthorized access to our servers and encrypted all data on the servers.

The external technical advisers have concluded that the criminals have gained access, via a stolen password from one of our customers and using the IP-address of the customer, to the Techotel IT-network and then from inside the network, they used specially designed software to attack the security barriers of the servers.

At the same time, we received information from the criminals with a ransom demand to be paid to access a decryption software key.

We immediately launched an attempt to remedy the situation by contacting a consultancy firm that are experts in handling communication and negotiations with the criminals in these circumstances. Their experience in these circumstances is vast as the number of such attacks has exploded all over the world and the criminals have developed extremely advanced technology to carry out the attacks with.

It became clear to us quickly that we had two options. Either accept that access to Picasso and all customer data could not be restored within a reasonable period of time if specialist companies would have to try to crack the encryption or agree to pay a ransom to ensure our customers' access to Picasso and data.

It is our clear basic position that one should not bow to criminals' demands for ransom, but the consideration for our customers and their companies made us choose to agree to pay a significant amount to the criminals. This occurred on June 10, 2021.

We received software that was supposed to decrypt data, but found that the received software did not work properly. There has been a dialogue with the criminals to solve the problems, and we also sought assistance from the universally recognised Norwegian company IBAS, who have world-class expertise in data recovery.

At the same time, all our servers have been re-installed, virus-scanned, updated etc.

We are very pleased to note that almost all our customers has access to Picasso etc. Unfortunately, some customers still experience some limitations in the access, however we are working 24/7 to solve these issues. You can find updated information on “operation info”.

We would very much like to thank our customers for their patience in connection with the criminals' hacker attacks. We have tried not only to remedy the situation as soon as possible, but also to keep our customers informed about the situation. We would also like to thank you for the many kind and understanding comments we have received in connection with this assault, not only on Techotel, but also our customers.

For the sake of good order, we made a notification to the Danish Data Protection Agency on 12 June 2021. It was subsequently agreed with the Danish Data Protection Agency that the individual customers did not need to make independent notifications, as Techotel would submit customer lists to the Danish Data Protection Agency. This would include all non-Danish EU based hotels also.

This agreement appears on the Danish Data Protection Agency's website:

Reviewer Re. AK Techotel

The Danish Data Protection Agency has become aware that there has been a breach of personal data security at the company AK Techotel last week. It is agreed with the data controller of Techotel that they report the security breach on behalf of all the data controllers who are affected by the security breach. The individual data controllers thus do not have to send a report of the security breach in question.

Anmeldelser vedr. AK Techotel

Datatilsynet er blevet bekendt med, at der er sket et brud på persondatasikkerheden hos virksomheden AK Techotel i sidste uge. Det er aftalt med databehandleren, at de anmelder sikkerhedsbruddet på vegne af alle de dataansvarlige, der er berørt af sikkerhedsbruddet. De enkelte dataansvarlige skal således *ikke* selv sende en anmeldelse af det pågældende sikkerhedsbrud.

We are looking forward to being back to normal business and putting this criminal attack behind us all.

Should you have any questions, not being answered by the information or “operation info”, please do not hesitate to contact us.