Vlissingen, [datum] april 2022

Onderwerp: datalek

Beste huurder,

l’escaut heeft te maken gehad met een digitale aanval, een hack. Gegevens van een aantal huurders zijn mogelijk ingezien of te koop aangeboden door de daders. Als u bent aangemeld voor onze nieuwsbrief Rondom Wonen, stuurden wij u hierover een mail op 30 maart en 5 april. Misschien hoorde u erover op Omroep Zeeland of las u er iets over in de krant.

**In deze brief leest u het laatste nieuws**
De adresgegevens van onze huurders kunnen we gelukkig weer gebruiken. We zijn blij dat we u deze brief sturen met het laatste nieuws.

**Er is een datalek van uw gegevens**

Dat betekent dat de daders bij de digitale aanval uw persoonsgegevens (deels) hebben ingezien, opgeslagen of verspreid.

Zoals we nu weten, gaat het vooral om de volgende gegevens:

* Naam
* Adresgegevens
* E-mailadres
* Telefoonnummer

**U hoort van ons als er ook andere gegevens van u gelekt zijn**

Op dit moment lijkt het erop dat er geen andere gegevens van huurders zijn gelekt. Dit onderzoeken we uiteraard verder. Mocht dit helaas wel het geval zijn, dan informeren we u hierover rechtstreeks uiterlijk 1 juni 2022. Hoort u niets van ons, dan zijn er géén andere gegevens van u gelekt.

**Wij maakten een eerste melding bij de Autoriteit Persoonsgegevens**

Dit hebben we gedaan omdat de daders van de digitale aanval niet het recht hebben om deze persoonsgegevens in te zien, op te slaan of te verspreiden. Deze melding vullen we verder aan met de informatie die bij ons bekend wordt.

**We hebben direct actie ondernomen om de systemen en gegevens veilig te stellen**

Zodra we merkten dat onze systemen gehackt waren, hebben we actie ondernomen. We werken continu aan het verbeteren van de beveiliging van persoonsgegevens en aan het tegengaan van de gevolgen van een datalek.

**Het is belangrijk dat u alert bent!**
We weten dat de gestolen persoonsgegevens zijn aangeboden via een speciale website. Maar we weten niet óf en hoe oplichters gestolen persoonsgegevens gaan gebruiken. Niet alle datalekken maken identiteitsfraude mogelijk. Met losse gegevens kan een fraudeur niet veel. Dit kan wel met een combinatie van gegevens. Daarom vragen we u om de komende tijd extra goed op te letten voor valse mails, sms'jes of valse telefoongesprekken.

**Zo kunt u nepberichten (phishing) herkennen**

* U wordt gebeld door een voor u onbekend nummer en de beller vraagt om persoonsgegevens. Of de beller biedt aan u te helpen door op afstand via uw computer mee te kijken. Trap hier niet in. Stel vragen, wees kritisch en hang direct op als u het niet vertrouwt. Bel eventueel terug naar een algemeen telefoonnummer van de organisatie en controleer of zij u belden.
* Klik niet zomaar op links in mails of sms/whatsapp berichten. Lees wat er staat en controleer de website op internet.
* Vaak word je onder druk gezet. In het bericht wordt aangegeven dat als je niet snel reageert, bijvoorbeeld uw bankrekening zal worden geblokkeerd. Dit is een teken dat er iets niet klopt.
* Vraagt een familielid of vriend u via WhatsApp om (afwijkende) hulp? Bijvoorbeeld voor het overmaken van een geldbedrag? Zorg dan dat u altijd met deze persoon in contact bent. En stel vragen die alleen deze persoon kan beantwoorden. Er wordt vaak iets ongebruikelijks gevraagd, zoals inloggegevens, een betaling enzovoort. Geef nooit zomaar gegevens.

**Bekijk ook eens deze handige websites**

* Op de website [www.haveibeenpwnd.com](http://www.haveibeenpwnd.com/) kunt u controleren of en zo ja waar en wanneer uw e-mailadres of telefoonnummer bij een datalek openbaar zijn geworden. U ziet dan meteen welke gegevens nog meer van u zijn gelekt en bij welk bedrijf. Het is verstandig om op die websites je inloggegevens te veranderen. [www.haveibeenpwned.com](http://www.haveibeenpwned.com/) wordt door fraudebestrijders beschouwd als een veilige website. Ook de Fraudehelpdesk adviseert deze website.
* Op [www.fraudehelpdesk.nl](https://www.fraudehelpdesk.nl/) vindt u nog meer tips over hoe u kunt voorkomen dat er misbruik wordt gemaakt van uw gegevens.
* Op [www.rvig.nl](https://www.rvig.nl/) kunt u identiteitsfraude melden en ondersteuning krijgen.

**Meer informatie**
Op onze website [www.lescaut.nl](http://www.lescaut.nl) vindt u meer informatie over de digitale aanval op onze systemen. Ook vindt u daar de brief die wij eerder al naar onze huurders stuurden.

**Het spijt ons erg dat dit gebeurd is**

We doen er veel aan om uw gegevens goed te beveiligen. Toch hebben we helaas niet kunnen voorkomen dat dit is gebeurd. Ik bied hiervoor mijn excuses aan.

**Heeft u een vraag? Bel ons**
Helaas zijn wij nog niet goed te bereiken via de mail. Daarom zijn wij telefonisch bereikbaar op nummer (0118) 42 23 00. U krijgt dan iemand aan de lijn van onze telefoonservice die uw gegevens noteert. Wij bellen u dan zo spoedig mogelijk terug.



Met vriendelijke groet,

Jan Leo van Deemter
directeur-bestuurder