Met betrekking tot de **AVG** (**A**lgemene **V**erordening **G**egevensbescherming), welke op 25 mei 2018 van kracht is geworden, zijn de volgende punten van belang. Op basis van deze punten is binnen Happy Days de verwerking, vastlegging en bewustwording in het kader van de AVG geborgd.

Happy Days NH, gevestigd aan Industrieweg 48a, 1613KV Grootebroek, is verantwoordelijk voor de verwerking van persoonsgegevens zoals weergegeven in deze privacyverklaring.

Contactgegevens

www.happydays-nh.nl
Industrieweg 48a
1613KV Grootebroek
Tel: 0228-521113

Dhr Lieuwe de Jong is de Functionaris Gegevensbescherming van Happy Days NH.
Hij is te bereiken via info@happydays-nh.nl

Persoonsgegevens die wij verwerken

Happy Days NH verwerkt uw persoonsgegevens doordat u gebruik maakt van onze diensten en/of omdat u deze zelf aan ons verstrekt.

Hieronder vindt u een overzicht van de persoonsgegevens die wij verwerken:
- Voor- en achternaam
- Geslacht
- Geboortedatum
- Geboorteplaats
- Adresgegevens
- Telefoonnummer
- E-mailadres
- Bankrekeningnummer

Bijzondere en/of gevoelige persoonsgegevens die wij verwerken

Onze website en/of dienst heeft niet de intentie gegevens te verzamelen over websitebezoekers die jonger zijn dan 16 jaar. Tenzij ze toestemming hebben van ouders of voogd. We kunnen echter niet controleren of een bezoeker ouder dan 16 is. Wij raden ouders dan ook aan betrokken te zijn bij de online activiteiten van hun kinderen, om zo te voorkomen dat er gegevens over kinderen verzameld worden zonder ouderlijke toestemming. Als u er van overtuigd bent dat wij zonder die toestemming persoonlijke gegevens hebben verzameld over een minderjarige, neem dan contact met ons op via info@happydays-nh.nl, dan verwijderen wij deze informatie.

Met welk doel en op basis van welke grondslag wij persoonsgegevens verwerken

Happy Days NH verwerkt uw persoonsgegevens voor de volgende doelen:
- Het maken van reserveringen en sturen van bevestigingen per e-mail
- Het afhandelen van uw betaling (eventuele rekeningen op factuur verzenden per e-mail)
- Verzenden van onze nieuwsbrief en/of reclamefolder
- U te kunnen bellen of e-mailen indien dit nodig is om onze dienstverlening uit te kunnen voeren
- U te informeren over wijzigingen van onze diensten en producten

Hoe lang we persoonsgegevens bewaren

Happy Days NH bewaart uw persoonsgegevens niet langer dan strikt nodig is om de doelen te realiseren waarvoor uw gegevens worden verzameld. De Autoriteit Persoonsgegevens bewaart de persoonsgegevens welke u invult op ons reserveringsformulier volgens de meldplicht datalekken 7 jaar. Ook wij hanteren bewaartermijn van 7 jaar voor alle persoonsgegevens.

Delen van persoonsgegevens met derden

Happy Days NH verkoopt uw gegevens niet aan derden en verstrekt deze uitsluitend indien dit nodig is voor de uitvoering van onze overeenkomst met u of om te voldoen aan een wettelijke verplichting. Met bedrijven die uw gegevens verwerken in onze opdracht, sluiten wij een bewerkersovereenkomst om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van uw gegevens. Happy Days NH blijft verantwoordelijk voor deze verwerkingen.

Cookies, of vergelijkbare technieken, die wij gebruiken

Happy Days NH gebruikt geen cookies of vergelijkbare technieken.

Gegevens inzien, aanpassen of verwijderen

U heeft het recht om uw persoonsgegevens in te zien, te corrigeren of te verwijderen. Daarnaast heeft u het recht om uw eventuele toestemming voor de gegevensverwerking in te trekken of bezwaar te maken tegen de verwerking van uw persoonsgegevens door Happy Days NH en heeft u het recht op gegevensoverdraagbaarheid. Dat betekent dat u bij ons een verzoek kunt indienen om de persoonsgegevens die wij van u beschikken in een computerbestand naar u of een ander, door u genoemde organisatie, te sturen.

U kunt een verzoek tot inzage, correctie, verwijdering, gegevensoverdraging van uw persoonsgegevens of verzoek tot intrekking van uw toestemming of bezwaar op de verwerking van uw persoonsgegevens sturen naar info@happydays-nh.nl.

Om er zeker van te zijn dat het verzoek tot inzage door u is gedaan, vragen wij u een kopie van uw identiteitsbewijs met het verzoek mee te sturen. Maak in deze kopie uw pasfoto, MRZ (machine readable zone, de strook met nummers onderaan het paspoort), paspoortnummer en Burgerservicenummer (BSN) zwart. Dit ter bescherming van uw privacy. We reageren zo snel mogelijk, maar binnen vier weken, op uw verzoek.

Happy Days NH wil u er tevens op wijzen dat u de mogelijkheid heeft om een klacht in te dienen bij de nationale toezichthouder, de Autoriteit Persoonsgegevens. Dat kan via de volgende link: https://autoriteitpersoonsgegevens.nl/nl/contact-met-de-autoriteit-persoonsgegevens/tip-ons

Hoe wij persoonsgegevens beveiligen

Happy Days NH neemt de bescherming van uw gegevens serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Als u de indruk heeft dat uw gegevens niet goed beveiligd zijn of er aanwijzingen zijn van misbruik, neem dan contact op met onze klantenservice of via info@happydays-nh.nl

Geautomatiseerde besluitvorming & Extra uitleg/informatie

Er is in dit document de wijze van melden van datalekken opgenomen en het privacy statement betreffende de vastlegging van persoonsgegevens

1. Bewustwording: impact van misbruik, risico, vastlegging en discipline
2. Rechten betrokkenen: gegevens welke vastgelegd zijn, mogen door betrokkenen worden opgevraagd, ingezien en desgevraagd worden verwijderd
3. Overzicht verwerking: Vastleggen van de verwerking van de gegevens en de stappen hierin. Tevens vastleggen met welke partijen en organisaties gegevens worden gedeeld en op welke wijze deze de gegevens verwerken en beschermen
4. Data Protect Impact Assessment: op welke wijze worden privacy risico's in kaart gebracht, welke risico's zijn er en hoe worden deze aangepakt c.q. verminderd
5. Privacy by design /Privacy by default: bij het in gebruik nemen van nieuwe systemen rekening houden met de bescherming van de gegevens / alleen die gegevens vastleggen die noodzakelijk zijn voor het systeem. Indien extra gegevens vastgelegd worden, dan een uitdrukkelijke toestemming van de gebruiker
6. Meldplicht: indien gegevens openbaar worden gemaakt, misbruik, data lek, dan dient hiervan melding gemaakt te worden. Opstellen van een procedure voor het melden
7. Verwerkersovereenkomsten: indien verwerking uitbesteed is, dan dienen de maatregelen van de verwerker bekend te zijn en dient een overeenkomst voor verwerking van de gegevens te worden opgesteld
8. Leidende toezichthouder: niet van toepassing, is van belang indien meerdere vestigingen aanwezig zijn
9. Toestemming; indien van toepassing dient toestemming te worden gevraagd van betrokkenen, dient een eenduidige wijze van toestemming opgesteld te worden met de noodzakelijke punten

Betreffende bovenstaande, zijn de volgende wijzigingen doorgevoerd in de huidige processen, informatievoorziening en verwerking van gegevens :

- Bevestigingen, rapportages en overzichten zijn voorzien van melding van de wijze van vastlegging van gegevens en/of verwijzing naar verwerking van gegevens. Tevens is hierin opgenomen op welke wijze gegevens gewijzigd dan wel verwijderd kunnen worde
- Op kassabonnen en transacties is een verwijzing opgenomen naar een pagina op de website voor toelichting van de verwerking van gegevens alsmede de uitleg van wijzigen en verwijderen van persoonsgegevens
- Op de website is de cookie melding aangepast aan de eisen welke hieraan worden gesteld in het kader van de AVG
- In de organisatie is een verantwoordelijke aangesteld voor naleving en handhaving van de AVG. Tevens is deze persoon bekend met de interne procedures alsmede de verwerking van de gegevens bij externe partijen (Naam:)
- Op basis van de verwerking en vastlegging van de gegevens zijn de volgende risico's in kaart gebracht met daarbij de maatregelen voor beperking:
  1. Openbaar worden van gegevens bij externe partijen
     - Maatregel: de gegevens welke bij externe partijen worden opgeslagen ofwel worden aangeleverd, zijn beperkt tot de gegevens welke voor specifieke doelen benodigd zijn en worden na gebruik verwijderd
     - Gegevens welke voor lange termijn bewaard moeten blijven bij externe partijen, worden in een afgeschermde omgeving beheerd (Lightspeed)

2. Reserveringssysteem: het reserveringssysteem is een lokaal systeem waarbij toegang tot het systeem verleend is aan de geautoriseerde medewerkers. Bij een datalek (in welke vorm dan ook) zal de toegang beperkt worden tot administrator rechten en zal melding gemaakt worden van de gegevens welke, indien bekend, openbaar zijn geworden. Tevens zullen de betrokkenen op de hoogte worden gebracht
3. Lijsten / Overzichten met persoonsgegevens: toegang tot lijsten en overzichten waar gegevens van personen worden bijgehouden, is beperkt tot medewerkers welke deze in het kader van haar/zijn functie nodig hebben.
4. Website: persoonsgegevens welke op de website worden verzameld, worden niet op de server opgeslagen; deze gegevens worden direct lokaal verwerkt en vastgelegd indien dit in het kader van de reserveringen of aanvragen benodigd is.

Partijen welke persoonsgegevens aangeleverd krijgen, dan wel verwerken, zijn:

- Lightspeed: AVG is afgeschermd en geborgd binnen Lightspeed
- Web site: is in beheer van Mprompt, worden geen persoonsgegeven opgeslagen

Datalek/Inbreuk

Bij een datalek gaat het om toegang tot of vernietiging, verlies, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens, en verlies van (toegang tot) persoonsgegevens.

De term ‘datalek’ komt niet voor in de wet. In de plaats daarvan heeft de Algemene verordening gegevensbescherming (AVG) het over een ‘inbreuk in verband met persoonsgegevens’.

Hiervan is sprake bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (Artikel 4, punt 12, AVG).

Categorieën datalekken
Er zijn drie categorieën datalekken te onderscheiden:

- *Inbreuk op de vertrouwelijkheid*
  Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.
- *Inbreuk op de integriteit*
  Wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.
- *Inbreuk op de beschikbaarheid*
  Wanneer er sprake is van een onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van, persoonsgegevens.
-

Een datalek kan, afhankelijk van de omstandigheden, in meer dan één van deze drie categorieën vallen.

Voorbeelden datalekken
Voorbeelden van datalekken zijn:

- het verlies van een USB-stick met niet-versleutelde persoonsgegevens;

- een cyberaanval waarbij persoonsgegevens zijn buitgemaakt;
- een besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn gemaakt.

Melding Misbruik/Datalek
Het melden van misbruik van persoonsgegevens, zal gedaan worden aan de hand van de meldplicht welke hier beschreven is

Meldplicht datalekken
De meldplicht datalekken houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).
Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie.

Meldplicht datalekken onder de AVG
De meldplicht datalekken geldt in Nederland al sinds 2016. Onder de nieuwe Europese privacywet die sinds 25 mei 2018 geldt, de Algemene verordening gegevensbescherming (AVG), blijft de meldplicht datalekken bestaan.
De AVG stelt wel strengere eisen aan de registratie van de datalekken in een organisatie. Organisaties moeten alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of zij aan de meldplicht datalekken hebben voldaan.

Datalek melden
Organisaties die een datalek willen melden bij de AP, kunnen dat doen via het meldloket datalekken (https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0).
In het privacystatement formulier meldplicht datalekken staat hoe de AP omgaat met de persoonsgegevens van degene die een datalek meldt.

Privacy Statement formulier meldplicht datalekken

Verantwoordelijke
De Autoriteit Persoonsgegevens is de zogeheten verwerkingsverantwoordelijke in de zin van de Algemene verordening gegevensbescherming (AVG). Dit houdt in dat de Autoriteit Persoonsgegevens beslist welke persoonsgegevens worden verwerkt, met welk doel dat gebeurt en op welke manier.
De Autoriteit Persoonsgegevens is er verantwoordelijk voor dat uw persoonsgegevens in overeenstemming met de AVG en op behoorlijke en zorgvuldige wijze worden verwerkt.

Persoonsgegevens
De Autoriteit Persoonsgegevens verwerkt persoonsgegevens in de zin van artikel 4, sub 1, van de AVG. Persoonsgegevens zijn alle gegevens die informatie kunnen verschaffen over een geïdentificeerde of identificeerbare natuurlijke persoon.
De Autoriteit Persoonsgegevens gebruikt uw naam, adres, telefoonnummer en e-mailadres om contact met u te kunnen opnemen als we een vraag hebben over uw melding.

Grondslag van de verwerking
De Autoriteit Persoonsgegevens moet het gebruik van uw persoonsgegevens kunnen baseren op een van de grondslagen uit artikel 6 van de AVG. Op grond van dit artikel is het onder meer toegestaan

deze gegevens te verwerken als dat noodzakelijk is om een wettelijke verplichting na te komen die geldt voor de verantwoordelijke (artikel 6, onder c, van de AVG).
Een dergelijke wettelijke verplichting heeft de Autoriteit Persoonsgegevens op grond van artikel 33 van de AVG. Dit artikel stelt dat de verantwoordelijke de Autoriteit Persoonsgegevens 'zonder onredelijke vertraging en indien mogelijk uiterlijk 72 uur na vaststelling in kennis stelt van een inbreuk op de beveiliging van persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Beveiliging persoonsgegevens
Artikel 32 van de AVG verplicht de Autoriteit Persoonsgegevens om passende technische en/of organisatorische maatregelen te nemen zodat een passende beveiliging de verwerking van persoonsgegevens waarborgt zodat zij beschermd zijn tegen onder meer verlies van persoonsgegevens, onrechtmatige verwerking van persoonsgegevens of vernietiging van beschadiging van die persoonsgegevens.
Zo worden de (persoons)gegevens tijdens verzending versleuteld. En vindt de verzending van (persoons)gegevens plaats via een beveiligde verbinding.

Bewaartermijn persoonsgegevens
De Autoriteit Persoonsgegevens bewaart de persoonsgegevens die u invult op het formulier meldplicht datalekken 7 jaar.

Uw privacy rechten
U heeft recht op inzage in uw persoonsgegevens (artikel 15 van de AVG) en het recht om correctie of verwijdering van uw persoonsgegevens te vragen (artikel 16 en 17 van de AVG).

Als u wilt weten welke persoonsgegevens van u de Autoriteit Persoonsgegevens verwerkt, kunt u een schriftelijk inzageverzoek doen. De Autoriteit Persoonsgegevens behandelt uw verzoek binnen een redelijke termijn.

Blijkt dat uw gegevens onjuist, onvolledig of niet relevant zijn? Dan kunt u een aanvullend verzoek doen om uw gegevens te laten wijzigen of aan te vullen.

Vraagt iemand om inzage, dan moet de organisatie diegene op een duidelijke en begrijpelijke manier laten weten:

- of de organisatie zijn persoonsgegevens gebruikt;
- wat het doel is van het gebruik;
- om welke gegevens/categorieën van gegevens het gaat;
- aan wie de organisatie de gegevens eventueel heeft verstrekt of aan welke categorieën van ontvangers de gegevens zullen worden verstrekt;
- wat de periode is waarin de persoonsgegevens naar verwachting zullen worden opgeslagen of in elk geval de criteria om die termijn te bepalen;
- dat de betrokkene verschillende rechten heeft (rectificeren, wissen, beperken van de verwerking, bezwaar maken tegen de verwerking e.d.);
- dat de betrokkene het recht heeft een klacht in te dienen bij de AP
- wat de herkomst is van de gegevens, als deze bekend is en de gegevens niet bij de betrokkene zijn verzameld;

- of sprake is van geautomatiseerde besluitvorming inclusief profilering met vermelding van de onderliggende logica en het belang en de verwachte gevolgen van die verwerking voor betrokkene.

Reikwijdte inzagerecht

Het recht op inzage betreft alleen inzage in iemands eigen gegevens. Mensen hebben dus geen recht op informatie over anderen.

Gebruikt een organisatie persoonlijke werkaantekeningen als geheugensteuntje? Dan vallen deze aantekeningen niet onder het inzagerecht.

Maar slaat de organisatie de aantekeningen vervolgens op in een dossier of verstrekt de organisatie deze aan anderen? Dan heeft degene over wie het gaat ook recht op inzage in deze aantekeningen.