Veiligheid data en privacy

Inleiding
Binnen DWSV worden gegevens van leden bewaard voor de ledenadministratie, inzet van vrijwilligers en deelname aan activiteiten. Daarnaast maakt DWSV ook gebruik van camera's om haar terreinen en opstallen te bewaken en elektronische sleutels voor toegang tot de terreinen en gebouwen (tags van SALTO). De gegevens die hierbij bewaard worden vallen onder de Algemene Verordening Gegevensbescherming (AVG). DWSV is daarom verplicht om inzichtelijk te maken welke gegevens zij bewaart, met welk doel, voor welke termijn en met wie zij gegevens deelt. Daarbij maakt DWSV onderscheidt tussen gerichte gegevens in het kader van de administratie en goede werking van de vereniging en het cameratoezicht. Natuurlijk geldt voor alle gegevens dat deze voldoende beveiligd moeten zijn tegen datalekken.

Administratie
Soort gegevens en bewaren van gegevens
DWSV bewaart van elk lid de in bijlage V1 genoemde gegevens voor de ledenadministratie.
De contactgegevens, geboortedatum en gegevens van de boot of boten zijn nodig voor plannen van ligplaatsen en stalling en het versturen van rekeningen. De foto van eigenaar met boot is nodig om ook op locatie eigenaar en boot te kunnen identificeren in geval van vragen of calamiteiten. Deze gegevens voor de ledenadministratie worden bewaard in E-captain (een online omgeving). Deze gegevens worden tot 10 jaar na het beëindigen van het lidmaatschap bewaard (gelijk aan de bewaarplicht voor onroerende zaken en BTW-vrijstelling, 7 jaar minimaal verplicht vanuit de belastingdienst voor debiteuren/crediteuren administratie).

DWSV verwerkt bovenstaande persoonsgegevens voor de volgende doeleinden:
- De naam, adres, telefoonnummer en/of e-mailadres van leden wordt gebruikt voor contact over het lidmaatschap en de eventuele opzegging daarvan, voor de verstrekking van de door het lid
- aangevraagde informatie of het afhandelen van de van het lid verkregen informatie.
- De namen, adresgegevens en telefoonnummer van leden wordt gebruikt voor het versturen van uitnodigingen, nieuwsbrieven en informatie over faciliteiten en activiteiten van DWSV. Afmelding voor de nieuwsbrief of mailing is ten aller tijden mogelijk via een reply op de nieuwsbrief of mailing.
- De naam en het bankrekeningnummer van leden wordt gebruikt om betalingen, bijv. van het lidmaatschapsgeld, cursussen, trainingen, bestellingen, afgenomen diensten af te wikkelen.

Voor de inzet van vrijwilligers wordt een aparte lijst gebruikt. Op deze lijst worden alleen gegevens bijgehouden die noodzakelijk zijn om vrijwilligers in te zetten. Dit zijn voor- en achternaam, telefoonnummer, mailadres en kenteken auto indien een ontheffing voor het Foppenpolderpad nodig is. De lijsten met vrijwilligers worden bewaard in Microsoft Teams. Deze worden regelmatig en minimaal 1x per jaar bijgewerkt. Op deze lijst staan alleen de actieve vrijwilligers.

Voor stalling en registratie van de zelfwerkzaamheid worden in Teams lijsten bijgehouden met voor- en achternaam, naam boot (stallingslijst) en aanwezigheid op werkavonden/-ochtenden (zelfwerkzaamheid). De stallingslijst en aanwezigheidslijst voor de zelfwerkzaamheid wordt na gebruik direct verwerkt in E-captain en verwijderd.

Daarnaast wordt periodiek (ongeveer 1x per 2 jaar) aan alle leden gevraagd om in een googleforms-document aan te geven voor welke werkzaamheden men benaderd kan worden met voor- en achternaam. Deze inventarisatie is op basis van vrijwilligheid en wordt alleen gebruikt om gericht leden te benaderen voor verzoeken om deelname aan werkzaamheden. Bij een nieuwe uitvraag wordt de oude lijst verwijderd.

Toegang tot de gegevens
Elk lid kan zijn eigen gegevens in E-captain inzien en wijzigingen aanbrengen in de eigen contactgegevens. Alleen de daartoe gerechtigde personen (bestuur, ledenadministratie en voorzitters van de loodscommissie en havencommissie, terreinbeheerder en havenmeesters) kunnen gegevens van anderen inzien (in E-captain en in Teams) en deze wijzigingen. Deze personen mogen geen persoonsgegevens met andere leden of derden delen.

Leden kunnen via de secretaris van DWSV (secretaris@dwsv.nl) een verzoek indienen om de eigen persoonsgegevens in te zien, te wijzigen of verwijderen. Het bestuur van DWSV zal het verzoek in behandeling nemen en binnen een maand na ontvangst beantwoorden. Een verzoek tot het verstrekken van persoonsgegevens van een ander lid zal altijd geweigerd worden. Wel kan aangeboden worden om de contactgegevens van de vragende partij door te geven met verzoek contact op te nemen.

Indien een lid vragen heeft over, bezwaar wil maken tegen of een klacht heeft over de (verdere) verwerking van persoonsgegevens kan contact opgenomen worden met het bestuur van DWSV (bestuur@dwsv.nl).

Elektronische sleutels (SALTO-systeem)
Voor de toegangshekken en deuren op beide locaties wordt gebruik gemaakt van een
Het SALTO-systeem houdt log-data bij van de tags die gebruikte worden om een slot te openen (tagnummer, slot dat geopend wordt, datum en tijdstip). Omdat elke tag een uniek nummer heeft, welke is gekoppeld aan een lid, kan zichtbaar gemaakt worden op welk moment welk lid op welke locaties is of welk slot deze geopend heeft. Deze informatie wordt bewaard in de cloud van Amazon (salto.dwsv.nl) en kan alleen bekeken worden door de terreinbeheerder, bestuurslid locaties, voorzitter en tagbeheerder.

Cameratoezicht
DWSV zet cameratoezicht in om haar terreinen en opstallen te beschermen op de locaties Buitenwatersloot 346 te Delft en de jachthaven aan de Foppenhaven. Aangezien beide terreinen afgelegen of afgeschermd liggen van bewoonde gebieden ontbreekt voldoende toezicht. Het bestuur van de DWSV is, gelet op het bovenstaande, van mening dat er **een gerechtvaardigd belang** bestaat om toepassing van cameratoezicht te effectueren. De camera's zijn allen in het zicht gehangen en zijn gericht op het eigen terrein en opstallen. Het cameratoezicht is op de terreinen aangekondigd met borden "cameratoezicht". Camera's zijn hardwarematig voorzien van een mogelijkheid tot opname van geluid. Deze optie wordt nadrukkelijk niet toegepast.

Het primaire doel van het cameratoezicht is het beschermen van eigendommen van de DWSV en van haar leden tegen diefstal en vernieling. Enerzijds door de preventieve werking die uitgaat van duidelijk zichtbaar cameratoezicht (afschrikking). Anderzijds door, op vordering van politie of justitie, een aangifte van een dergelijk incident te kunnen onderbouwen en eventueel onderzoeksrichtingen te ondersteunen.

De camerabeelden worden alleen opgeslagen om in geval van een calamiteit terug te kunnen kijken en worden niet verwerkt of geanalyseerd. De camerabeelden worden bewaard op de beveiligde netwerkschijf en standaard gewist indien de schijf vol is, doch uiterlijk na 28 dagen. In geval van een calamiteit kan het bestuur van DWSV besluiten de beelden veilig te stellen voor nader onderzoek en langer te bewaren. In dat geval zal de ICT-beheerder op verzoek van het bestuur de camerabeelden apart opslaan. De camerabeelden mogen langer dan 28 dagen bewaard worden in het kader van een wettelijke bewaarplicht of als dat noodzakelijk is voor de afhandeling van een geconstateerd incident. Zodra het incident is afgehandeld worden de beelden vernietigd.

Het cameratoezicht geschiedt onder verantwoording van het bestuur van DWSV. Het bestuur is verantwoordelijk voor het beheer van het systeem. De ICT-beheerder en terreinbeheerder zijn belast met het dagelijks beheer van het systeem (de technisch beheerder).

De camerabeelden zijn slechts toegankelijk voor onderstaande functionarissen binnen DWSV en worden niet verstrekt aan derden (leden of niet-leden) of elders opgeslagen of gedeeld tussen genoemde functionarissen. Hoewel eenieder waarvan persoonsgegevens (beelden) zijn vastgelegd, op basis van de Algemene verordening gegevensbescherming (AVG), recht op inzage het recht heeft om de eigen gegevens in te zien kunnen camerabeelden niet opgevraagd worden door leden omdat niet uit te sluiten is dat op betreffende beelden ook andere personen staan, welke privacy beschermd moet worden. Beeldmateriaal wordt alleen aan de politie, justitie of enig ander bevoegde autoriteit overhandigd indien deze de beelden vordert via een officiële procedure of schrijven.

Lijst functionarissen:
Voorzitter bestuur
Bestuurslid locaties
Voorzitter loodscommissie
Voorzitter havencommissie
Terreinbeheerder
Havenmeesters
ICT-beheerder

Uitkomsten scan Data Protection Impact Assessment (DPIA)
- Bezoekers en leden worden gewezen op cameratoezicht;
- Camerabeelden worden niet verwerkt of geanalyseerd en zijn niet gekoppeld met databases;
- Er is geen sprake van gegevensverwerking, monitoring of analyse van persoonskenmerken;
- Er worden dor DWSV geen besluiten met rechtsgevolgen genomen op basis van de camerabeelden;
- Camerabeelden alleen kunnen nooit leiden tot het blokkeren van toegang tot de terreinen of andere rechten die leden hebben op grond van hun lidmaatschap;
- Hiermee is geen sprake van een hoog risico op de privacy en is een DPIA niet verplicht.

Cybersecurity

DWSV beheert zelf geen servers met data, maar bewaart deze in de cloud van E-Captain (data ledenadministratie en hosten website), Microsoft (Office en Teams) en Amazon (Salto-systeem).

De servers van E-captain en Microsoft zijn, naar eigen zeggen, goed beveiligd tegen hacken. Over mogelijke hack-aanvallen valt niet zoveel te zeggen. Om mogelijk misbruik van inloggegevens te voorkomen, maakt DWSV per 15 juni 2024 gebruik van MFA (Multi Factor Authentication). De website van DWSV bevat geen gevoelige data, maar biedt wel de mogelijkheid om in te loggen op een beperkt deel van E-Captain met gebruik van MFA. Met het implementeren van MFA is het risico op een datalek klein.

Het Salto-systeem voor de Tags draait op een intern netwerk. Zowel dit interne netwerk als Amazon zijn beschermd met MFA. De verbinding van Salto naar de buitenwereld gaat via VPN (naar de server) en via de Unifi firewall (naar de gebruikerskant). Dit zijn doortimmerde en vrij technische systemen met weinig gebruikers. De tag gebruikers blijven intern en vormen geen kwetsbaarheid. Het risico op een datalek is daarmee klein.

De beveiligingscamera’s zijn, op 2 na, bedraad aangesloten op een eigen subnet, de 2 onbedrade camera’s zijn via Wifi aangesloten op het subnet. Dit betekent dat toegang tot een camera geen toegang tot het netwerk geeft. De camera’s vallen verder ook onder de Unifi authenticatie met MFA en sterke wachtwoorden. Het risico op een datalek is daarmee klein.

Bijlagen

Bijlage V1: lijst met gegevens van leden in de ledenadministratie

Lid
lidnummer
Voor- en achternaam
Adres
Telefoonnummer
e-mailadres
Geboortedatum, geboorteplaats
geslacht
foto
facturen openstaand en voldaan (geen persoonsgevoelig gegeven)
bankgegevens
stallingplek (geen persoonsgevoelig gegeven)
Beroep/kennis of ervaring (geen persoonsgevoelig gegeven)
Werkavondverplichting voldaan ja/nee (geen persoonsgevoelig gegeven)
Nummer toegangstag

Boot
naam boot of boten (geen persoonsgevoelig gegeven)
afmetingen (geen persoonsgevoelig gegeven)
type boot (geen persoonsgevoelig gegeven)