torerne sammen med den liste, der er omhandlet i artikel 31, stk. 8.

Artikel 8

Udveksling af supplerende oplysninger

1. Supplerende oplysninger udveksles i overensstemmelse med »Sirene-Håndbogen« og ved hjælp af kommunikationsinfrastrukturen. Hvis kommunikationsinfrastrukturen ikke er til rådighed, kan medlemsstaterne anvende andre tilstrækkeligt sikrede tekniske midler til at udveksle supplerende oplysninger.

2. Supplerende oplysninger må kun anvendes til det formål, de blev meddelt til.

3. Anmodninger fra en anden medlemsstat om supplerende oplysninger besvares snarest muligt.

4. Der skal efter proceduren i artikel 51, stk. 2, vedtages detaljerede bestemmelser for udvekslingen af supplerende oplysninger i form af Sirene-Håndbogen, med forbehold af bestemmelserne i retsakten om oprettelse af forvaltningsmyndigheden.

Artikel 9

Overholdelse af tekniske krav

1. For at sikre en hurtig og effektiv overførsel af oplysninger skal hver medlemsstat ved oprettelsen af sin N.SIS II overholde de protokoller og tekniske procedurer, der er fastsat for at sikre, at N.SIS II er kompatibel med CS-SIS. Disse protokoller og tekniske procedurer fastsættes efter proceduren i artikel 51, stk. 2, jf. dog bestemmelserne i retsakten om oprettelse af forvaltningsmyndigheden.

2. Hvis en medlemsstat anvender en national kopi, skal den ved hjælp af de tjenester, som CS-SIS stiller til rådighed, sikre, at oplysninger lagret i den nationale kopi via automatiske ajourføringer, jf. artikel 4, stk. 4, er identiske og i overensstemmelse med SIS II-databasen, og at en søgning i dens nationale kopi giver et søgeresultat, der svarer til resultatet af en søgning i SIS II-databasen.

Artikel 10

Sikkerhed - medlemsstater

1. Hver medlemsstat vedtager i relation til sin N.SIS II de nødvendige foranstaltninger, herunder en sikkerhedsplan, med henblik på:

a) fysisk at beskytte oplysninger, bl.a. ved at udarbejde beredskabsplaner for beskyttelse af kritisk infrastruktur
b) at forhindre, at uautoriserede får adgang til de anlæg, der benyttes til behandling af personoplysninger (kontrol med fysisk adgang til anlæggene)
c) at forhindre, at databærerne kan læses, kopieres, ændres eller fjernes af uautoriserede personer (kontrol med databærere)
d) at forhindre uautoriseret indlæsning af oplysninger samt uautoriseret læsning, ændring eller sletning af indlæste personoplysninger (kontrol med optagelse)
e) at forhindre, at edb-systemerne kan benyttes af uautoriserede personer ved hjælp af datatransmissionsudstyr (brugerkontrol)
f) at sikre, at autoriserede personer, hvad angår brugen af et edb-system, kun får adgang til de oplysninger, som henhører under deres kompetence, og kun ved hjælp af individuelle og entydige brugeridentiteter og fortrolige password (adgangskontrol)
g) at sikre, at alle myndigheder med adgangsret til SIS II eller til anlæggene opretter profiler, der beskriver funktioner og ansvarsområder for de personer, som er autoriseret til at få adgang til, indlæse, ajourføre, slette og søge i oplysningerne, og øjeblikkelig stiller disse profiler til rådighed for de nationale tilsynsmyndigheder, omhandlet i artikel 44, stk. 1, på deres anmodning (personaleprofiler).
h) at sikre, at det er muligt at undersøge og fastslå, til hvilke myndigheder der kan videregives personoplysninger via datatransmissionsudstyr (kontrol med videregivelse)
i) at sikre, at det er muligt efterfølgende at undersøge og fastslå, hvilke personoplysninger der er indlæst i edb-systemerne, hvornår, af hvem og med hvilket formål (efterfølgende kontrol med indlæsning)
j) at forhindre uautoriseret læsning, kopiering, ændring eller sletning af personoplysninger i forbindelse med overførsel af oplysninger eller transport af databærere, navnlig ved